Bachelor's thesis

Bachelor of Engineering, Information and Communications Technology

2020

Perla Rocío Ramírez Sanabria

DIGITAL FORENSICS

– Guidelines and Tools for a Digital Evidence Investigation Process. A Case Study for a Business Data Leak

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Engineering, Information and Communications Technology

2020 | 45, 79

Perla Rocío Ramírez Sanabria

DIGITAL FORENSICS

- Guidelines and Tools for a Digital Evidence Investigation Process. A Case Study for a Business Data Leak

The objective of this thesis was to provide a suitable and admissible analytical framework for a digital forensic analysis carried out by an investigator. In this thesis these concepts are explained in-depth to provide what could be considered as a guide for the execution of a digital evidence investigation. It is important to note that this investigation can usually, or rather must, end in a judicial process.

The theoretical framework of this thesis has been developed by consulting books written by specialists in the field of digital forensics, ISO/IEC standard documents, as well as models described by different government organizations and user guides for the required tools. In the case study, the concepts explained previously are exposed in the case of an insider threat performing a data leak to a company in the competition. After performing the analysis of the evidence acquired for the case, it was possible to determine that a data breach performed by an insider threat took place. The results of the practical analysis are decisive in a judicial court if the procedures of the analysis have been followed, hence the importance of the proper application of the methods and use of the tools.

KEYWORDS:

Digital Forensics, Cybersecurity, Expert Examiner, Investigation, Digital Evidence, Cybercrime

CONTENTS

APPENDICES

FIGURES

TABLES

LIST OF ABBREVIATIONS

IETF Internet Engineering Task Force

ISO/IEC International Standard Organization/ International Electrotechnical Commission

RFC Request for Comments

1 INTRODUCTION

Throughout history, communications users have evolved as well as their need to reach longer distances and wider audiences. To that end, computing was born and later the Internet, a technology capable of communicating to millions of people around the world instantly which has become a tool indispensable to carry out daily actions.

The Internet is one of the most powerful tools society possesses nowadays and being able to access this resource carries a great responsibility. Internet users must be aware of the dangers that can be found on the Web.

Cybercrime constitutes one of the most important threats regarding information technology. The use of the Internet has been extended to almost every aspect of society's lives, whether the subject is a professional matter or private life. This is the reason why it entails the greatest threat to every user.

Now, more than ever, it is possible to share every kind of data with any kind of device. Data include as files or media in any shape or form by using laptops, mobile phones, personal computers, and a long list of different devices. The information transmitted can be intercepted, manipulated, or deleted and the user must be aware of the nature of the information shared as well.

It is difficult, given these advances and continuous changes, to find updated bibliography that compiles: the latest versions of forensic software, the new legislative orders, recent standards and norms published, and other content disclosed by associations, schools, and agencies.

The theoretical framework of this thesis has been developed by consulting books written by specialists in the field of digital forensics, ISO/IEC standard documents, as well as models described by different government. The documentation for the practical framework was based on software user guides as well as training offered by the developers.

The purpose of this work is to offer an updated reference document, of a theoretical and practical nature, with the technical-legal aspects that the future forensic computer expert must know, and to provide an introductory look at the hardware and software technology used in the digital forensic investigation.

The thesis focuses mainly on the technical aspects of the analysis. This includes the description of the investigation process as well as the tools and techniques. The reason behind this point of view is the jurisdiction of laws. Every country has different legislation regarding different crimes.

Chapter 2 explains the basic concepts related to digital evidence. These include its definition, principles, characteristics as well as the importance of the chain of custody from the beginning to the end of the investigation.

Chapter 3 encompasses the broad concept of a "Digital evidence Investigation Process", where the recommended steps in each phase of the process are discussed in detail. The model explained is the NIJ 2004 model - which has been written and published by the United States Institute of National Justice. This is a globally accepted model. In addition,

internationally applicable methodologies have been cited and described, being mostly developed by ISO/IEC and IETF.

Chapter 4 describes the different tools used to carry out the analytical process. Software solutions are explained. The explanations detail the installation processes, the different features present the format options that users have. The description of these tools arises from the reading of the different documentation guides made available by the developers. When explaining certain tools in depth, it has been decided to describe open source tools, to guarantee easy access to them.

Moreover, it describes the hardware solutions, including among these the workstations used to carry out the investigation as well as certain tools used mainly in the evidence acquisition phase. These tools have been explained in less depth due to the lack of resources to be able to use them in the practical case. It has been chosen to introduce the products briefly and include the data sheet in the appendices to record their specifications.

In the last chapter, the theoretical concepts and knowledge discussed in previous chapters are put into practice by carrying out a complete practical case of digital forensic investigation and analysis. Each phase of the investigation is illustrated with images and screenshots, the programs and tools used are described, the results obtained based on the requirements of the judicial file are discussed, and finally, the conclusions are drawn up..

The choice of topic has been based on the interest of the author of the thesis, in addition to the need for an expansion of knowledge within the framework of cybersecurity.

1.1 Cybercrime

According to the definition in (Panda Security, 2018) cybercrime is:

"Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device. It is also a cybercrime to sell or elicit the above information online."

It is also important to remark that there is a possibility for a computer to be a tool and a target at the same time, as it occurs in the case of hacking.

In the context of cybercrime there exist several subgroups like "Cyber-terrorism", "information welfare", "phishing", "spams", "denial of service attacks", "hacktivism", "hate crime", "identity thefts", "online gambling" [1] as well as the production and distribution of child pornography as it is noted in (Wall, 2009)

Also, besides the different subgroups mentioned above, there are three major categories where cybercrime falls into as is described in (Panda Security, 2018):

[1] Legal in many countries. It may end up in scams and it might be easily accessible by underage individuals

- **Property cybercrime:** refers to the possession of an individual's personal information such as credit card information or login credentials. This information can be used with malicious intent for instance identity theft, making fraudulent online purchases, or gain access to online bank accounts.
- **Individual cybercrime:** refers to the distribution of malicious or illegal information. This can include cyberstalking, distribution of pornography, or trafficking.
- **Government cybercrime:** refers to what it is known as cyber terrorism and it comprises hacking of government sites, military websites, or distribution of propaganda.

1.2 Digital Forensics

According to information found in (Sant & Hewling, 2011) digital forensics refers to the acquisition, preservation, analysis, and representation of digital evidence produced from the investigation of digital-related crimes. This analysis digs deep into performing with certain specialized techniques, procedures, and tools that are going to be discussed later in the thesis. Digital forensics, which can also be referred to as "Computer Forensics", can be explained as "the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications and storage devices. A forensic specialist must collect data in such a way that is admissible as evidence in a court of law." (Vacca & Rudolph, 2010)

Digital Forensics will serve as a tool to pursue cybercrime in all categories mentioned in the section above. As cybercrime grows exponentially every day, evidence of such felonies grows as well. This is the reason why professionals that work in this field need to be aware of two important facets: technology and law. The experts, besides being proficient in the latest tools and methods for digital forensics analysis, need to be up to date with subjects such as information security, cybercrime, and cybersecurity as well as the judicial system regarding forensics in this matter. Computer Forensics incorporates the experience of IT, forensics, and legislation which poses a fascinating and daunting range of problems surrounding cybersecurity to be addressed. Cybercrimes impose new challenges when it comes to their prevention, detection, investigation, and prosecution.

For an analysis to be perfectly carried out, there are several methods with different steps and characteristics that will guarantee the digital evidence to be preserved to ensure authenticity, traceability, and auditing in processes. "The traceability and preservation of processes is an important aspect to verify and guarantee the authenticity of all the digital objects used and produced by the process, and to allow an analysis whether the processes were executed as expected, or according to regulations". (Mayer, et al., 2014)

Digital Forensics can be used in several settings according to (Sammons, 2012):

- **Criminal Investigations:** In the context of criminal investigation a vast number of crimes can be included such as child pornography, identity theft, homicide, sexual assault, robbery and burglary. The main reason behind this is that any of these crimes can still leave a digital evidence. In modern days, almost every device possessed by a citizen can provide such evidence.

- **Civil Litigations:** In civil cases, both parties require to examine evidence that is going to be used against them. This legal process is known as "discovery". Previously, this discovery involved the examination of each party exchanging reports, letters, and memos; however, the introduction of digital forensics and eDiscovery [2] has greatly changed this practice.
- **Intelligence:** Terrorists and foreign governments have also joined the digital era. It is known that nowadays terrorists use digital technologies as a tool to communicate, recruit, and plan attacks.
- **Administrative Matters:** Digital evidence can also be profitable "incidents other than litigation and matters of national security. Violations of policy and procedure often involve some type of electronically stored information, for example, an employee operating a personal side business, using company computers while on company time."

[2] "As part of a process known as Electronic Discovery (eDiscovery), digital forensics has become a major component of much high dollar litigation. eDiscovery “refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case” (Sammons, 2012)

2 DIGITAL EVIDENCE

Digital evidence is defined as *any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi* (adapted from (Chisum, 1999)).

There are several other definitions such as the one proposed by the Standard Working Group on Digital Evidence (SWGDE), which states that any information of probative value that is either stored or transmitted in a digital form. Another definition proposed by the International Organization of Computer Evidence (IOCE) is information stored or transmitted in binary form that may be relied upon in court. (Casey, 2011)

As previously mentioned in Chapter 1, the data shared through networks can be in any shape or form. Different devices, produce different types of data. As this occurs, it is normal to expect different sources of evidence, which can be seen in Table 1.

Table 1. Sources of Digital Evidence (Jhala, n.d.)

Sources	Devices	Potential Evidence
Storage Devices	Hard Drives, External Hard Drives, Memory Cards, Removable Media, Thumb Drives	E-mail messages, Internet browsing history and chat logs, photographs, image files, databases, financial records and event logs.
Handheld Devices	Mobile Phones, Tablets	Software applications, data, documents, Internet browsing history and chat logs, photographs, image files, databases, financial records
Peripheral Devices	Keyboard and mouse, Microphones, Web cameras, Memory card readers, VoIP devices, Printers	Incoming and outgoing phone and fax numbers; recently scanned, faxed, or printed documents; and information about the purpose for or use of the device.
Network Devices	Network hub, Laptop network card and ethernet cable, Internet modems, Network switch and power supply, Wireless access point, Wireless network server	The connected devices themselves. The device functions, capabilities, and any identifying information associated with the computer system; components and connections, including Internet protocol (IP) and local area network (LAN) addresses associated with the computers and devices; broadcast settings; and media access card (MAC) or network interface card (NIC) addresses
Others	Surveillance equipment, Digital Cameras, Video Cameras, Digital Audio Recorders, Video Game Consoles, GPS Systems	The device or item itself, its intended or actual use, its functions or capabilities, and any settings or other information it may contain is potential evidence.

2.1 Locard’s Principle

The Locard's Principle (Figure 1) states that any interaction between two items will create evidence. This will apply to any kind of interaction at a crime scene, "including between an offender and victim, between a person with a weapon, and between people and the

crime scene itself." (Casey, 2011). This will apply to both physical, which are out of the scope of this thesis, and digital evidence. Figure 1 illustrates the Locard's principle.

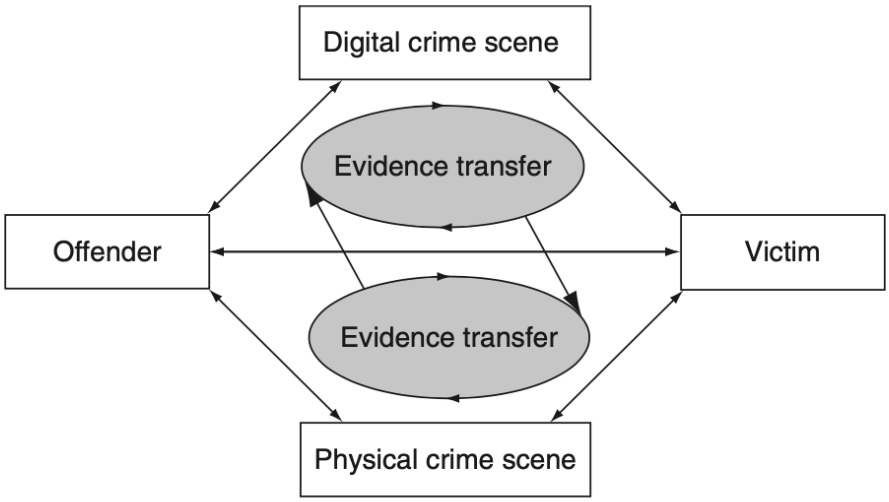


Figure 1. Graphical representation of the Locard's Principle (Casey, 2011)

2.2 Best Evidence Rule

When evidence constitutes writing, recording or photographs, the court can usually demand for the original version of the evidence. The reason behind this rule was that the decisions made in the courtroom were the best possible based on the best available information. "The policy behind the Best Evidence Rule is to prevent un-necessary inaccuracy stemming from the fallibility of human memory or transcription". (Ford, 2014)

Thanks to the rapid development in digital technologies such as photocopiers, scanners and computers it is easy to forge or alter evidence, but it is also available the exact replication of evidence. Generally, copies are accepted in place of the original, thus, "a genuine question is raised as to the authenticity of the original or the accuracy of the copy or under the circumstances it would be unfair to admit the copy in lieu of the original" (Casey, 2011). An advantage of presenting exact copies as evidence is that the original is prevented from being altered or damaged.

2.3 Hearsay

A piece of evidence might not be admitted if it contains hearsay. Considering that, if the speaker or author of said evidence is not present in the courtroom to prove its truthfulness, it is possible to revoke it.

"Evidence is hearsay where a statement in court repeats a statement made out of court in order to prove the truth of the content of the out of court statement. Similarly, evidence contained in a document is hearsay if the document is produced to prove that statements made in court are true. The evidence is excluded because the crucial aspect of the

evidence, the truth of the out of court statement (oral or documentary), cannot be tested by cross-examination." (Hoey, 1996)

This means that, for instance, some materials such as calls or e-mails can be used to prove the veracity of the evidence, but cannot be used to prove the full truth of the statements. Although, there are exceptions, which is the case for business records, this matter is out of the scope of this thesis.

2.4 Characteristics of Digital Evidence

Digital evidence must have certain characteristics along the process of forensics analysis:

- **Admissibility:** There must exist conformity with laws and legislative rules. A relationship between the digital evidence and the fact being proven must be established. Digital evidence must be obtained legally with authorization if necessary.
- **Integrity:** The source of the digital evidence must be trusted and remain unaltered from the time it was collected, by doing so the authentication process is supported. In order to verify the integrity of the evidence, digital fingerprints taken at the time of the collection and current state are compared.
  Message digests and cryptographic hash values are used in the process. The reason behind this is that message digest algorithms always produce the same value for a given input. Any slight change produces a different value, which can determine if the evidence has been altered since the time of the first hash value generation. Figure 2 illustrates the difference in MD5 output with two files that differ only in one character.

Digital Input	MD5 Output
The suspect's name is John	c52f34e4a6ef3dce4a7a4c573122a039
The suspect's name is Joan	c1d99b2b4f67d5836120ba8a16bbd3c9

Figure 2. Two files on a Windows machine that differ by only one letter have significantly different MD5 Values (Casey, 2011)

- **Completeness:** The digital evidence must help to lead the investigation to a conclusion. "When a forensic investigator states the evidence collected is a complete account it is implied that all the relevant evidence from the environment has been preserved (relevant to the subject of the investigation). We can interpret completeness as being the extent to which all the relevant evidence from the digital environment has been collected." (Ahmad & Ruighaver, 2004)
- **Authentication:** This concept refers to satisfying the court that the evidence has "remained unchanged, that the information in the record does in fact originate from its purported source, whether human or machine, and that extraneous information such as the apparent date of the record is accurate" (Sommer, 1997). The expert must be able to prove to the authenticity of the evidence by explaining the reliability of the computer equipment, the manner in which the basic data was

initially entered, the measures taken to ensure the accuracy of the data as entered, the method of storing the data and the precautions taken to prevent its loss of the reliability of the computer programs used to process the data, and the measures taken to verify the accuracy of the program.

Authentication is not a single-step process but, it is formed by two-step which are:

1. Initial examination of the evidence to determine if it provides what is claimed.
2. Closer analysis to determine its probative value.

- **Objectivity:** There must therefore be no bias when evaluating and providing data, this is crucial to provide decision makers with the clearest possible view of the facts. The most effective method is to encourage the proof to talk for itself as much as possible. Through inference and all the relevant empirical facts should be provided. The objective evaluation method which evaluates the findings of a forensic analyst for distinctions or some other deficiency is another efficient approach.
- **Repeatability:** A significant feature of the experimental process is that all tests or findings have to be replicated such that they can be confirmed independently. It is necessary to log in adequate detail the measures taken to identify and examine digital evidence to enable us to objectively validate the results in order to facilitate any analysis of forensic findings. (Prasad & Pandey, 2016)

2.5 Chain of Custody

According to the definition found in (Rios, 2014), the chain of custody "refers to the chronological documentation and/or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.". One the most important aspects of authentication is the maintenance and documentation of the chain of custody of evidence. Integrity and authenticity of a piece of digital evidence must be certified to a court of law (Benner, 2009). When evidence is presented as an exhibit, it is necessary to maintain and establish a record of the chain of evidence (Jaffee, et al., 2008). In case this record is not presented, the evidence may not have the characteristics needed even when its legitimate and unaltered (Tomlinson, et al., 2006). From the moment the evidence is collected and throughout the course of the investigation, the chain of custody keeps track of every individual that handles the evidence. This is performed in order to determine that the evidence was not manipulated or retained without authorization. Although there is no rule in regard to the amount of people that should intervene with the evidence, it is appropriate to keep this number as low as possible. Moreover, the people mentioned in the previous sentence must be qualified so evidence is handled properly to avoid tampering. (Badiye, et al., 2019)

3 DIGITAL EVIDENCE INVESTIGATION PROCESS

There are several models regarding digital investigation process. These process models have their origins in the early theories of computer forensics which defined the field in terms of a linear process. For example, forensic computing was described in 1999 by McKemmish as: "The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable". (McKemmish, 1999)

According to the citation above, the basis of a process will be constituted by the sequence of the following activities*, identification, preservation, analysis* and *reporting*. Variations will depend on the granularity and terminology of the different phases of said process. In the following subsections, the most common steps in the process are going to be discussed. Figure 3 illustrates the differente phases that exist in various digital investigation process models.

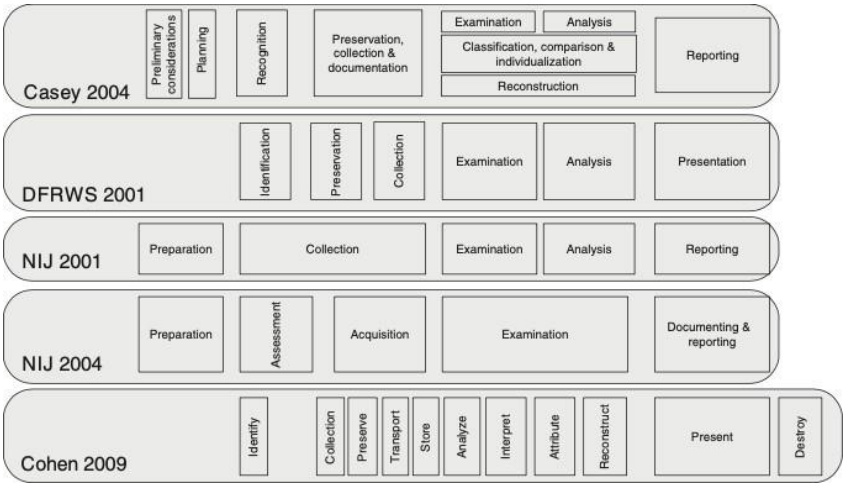


Figure 3. A comparison of terminology related to digital investigation process models. (Casey, 2011)

Preparation.

This activity consists in the generation of a plan of action. The main purpose of the plan is to effectively conduct the digital investigation by obtaining supporting resources and materials.

Survey/Identification.

In this step of the digital investigation, the main goal is to find potential sources of digital evidence, which can be any of the ones previously described in Table 1.

Preservation.

The fundamental objective in this step is to prevent any changes in the in-situ evidence. This is the step where the isolation of the system on the network, securitization of relevant log files and collection of volatile data occurs.

Examination and Analysis.

In this step, the experts search for and interpret the evidence found.

3.1 Phases

In the following subsections the different phases described by the NIJ 2004 model (U.S. Department of Justice Office of Justice Programs, 2004). It is crucial to note that this is only a model that describes possible and general guidelines surrounding the phases of the investigation. Later in the thesis, different standardised methods are going to be discussed and explained.

3.1.1 Evidence Preparation. Policy and Procedure Development

The objective is the development of policies and procedures to establish a plan of action with operations and functions to create the computer forensics unit. The plan of action must take into account several factors which are going to be discussed in the following sections:

Personnel

The digital forensics analysis must be carried out by competent experts, aware of the technologies to be in use, procedures and legislations. The subjects discussed by this segment include task requirements and

required qualifications, working hours, on-call status, command structure and team arrangements.

Administrative considerations

Software licensing The tools used by the experts in the analysis must be acquired legally and properly licensed by the agency.

Resource commitment A digital evidence investigation requires certain resources, financial and personnel. Within these resources, the following items are included: a facility where the analysis is going to take place, hardware equipment, software and hardware requirements, upgrades, experts' training and ongoing professional development and retention of examiners.

Training Throughout the investigation, expert examiners must stay skilled and up to date. This can be managed by improving the expertise of current workers or by hiring candidates from different disciplines. In the IT field, which is continuously evolving and changing, training is a crucial factor that must be considered in budget submissions.

Case management

The conditions for the prioritization and the scheduling of investigations will be determined and carried out once a proposal for forensic services is accepted. Criteria can include the complexity of the offense, court dates, deadlines, potential victims, legal factors, volatile nature of the evidence and resources available.

Evidence handling and retention

The guidelines for receiving, processing, documenting, and handling evidence and work products associated with the examination must be established according to the already existing departmental policy. Nevertheless, in the context of digital evidence handling and retention, the criteria could possibly exceed the policies mentioned before.

Developing technical procedures

There must be procedures to guide the process of evidence examination. This procedure must be put to test before applying it to ensure the potential results obtained are accurate, valid and reproducible. The procedures taken to carry out this part of the process begins with the identification of the problem. As it seems obvious, this step is mandatory to establish solution proposals to later test on samples. The results on the test can be positive or negative, this is rated after the evaluation. After all these tasks are performed, finalization of the procedure takes place.

3.1.2 Evidence Assessment

In order to decide the course of action, visual information will be cautiously examined concerning the complexity of the situation. The procedure of assessment will be executed by reviewing the search warrant or other legal authorization, the details of the case, the nature of the hardware and software, potential evidence and the circumstances surrounding the acquisition of the evidence. The assessment step is a key point in the investigation, without the potential collection and preservation of the evidence can be lost.

At this stage, the examiner evaluates the situation and considers many factors for analysis, such as whether the investigation should be conducted internally or involve an external agency; whether a search warrant should be issued. Any pre-search work may also be carried out such as the collection of details on the company's systems and assets; details on personnel participating in the situation, whether explicitly or indirectly; the collection of information on the protection incident team and its core skills, etc. In order to perform the inquiry the prosecutor must plan and test the forensic examination toolkit. The interviewer will also notify the testing team regarding the quest strategy and the recommendations.

There are two defined points within the assessment process, which are:

The evolution of this step is based on two main points, being the review of the case the first one. In this sub-step, the first task will be the identification of the legal authority for the forensic examination request. It is mandatory to have insurance of a completed

request for assistance. The subsequent tasks will be the completion of the documentation of the chain of custody. As was mentioned previously in the thesis, CoC is a crucial part of the investigation that must be kept updated overtime since the investigation is issued.

The second main point focus on the consideration of facts about the case. The first aspect an investigator should consider must be the processes that will be required to be performed on the evidence alongside the determination of the equipment needed. Inherently, this will lead to the possibility of the evidence. The evidence can issue from different sources. For instance, data obtained from an Internet service provider (ISP), remote locations or e-mail information. Peripheral devices (digital cameras, laminators, credit card blanks, check paper, scanners, and printers) can provide evidence to the case as well. After the investigator considers the sources of digital evidence, they should determine what can be considered actual evidence. Evidence can be found in media files, spreadsheets, document files, databases, financial records, aliases, e-mail accounts, e-mail addresses, ISP used, names, network configuration and users, system logs, passwords, usernames, etc. The skill levels of the users of these investigated devices need to be taken into account. This will determine if the user, being in possession of these skills, could have been able to conceal or destroy evidence with techniques such as encryption, booby traps, steganography. After all these aspects are evaluated, it is necessary to prioritize the order of evidence examination.

Onsite considerations

When investigators are onsite, there is a small window to consider the actions that need to be carried out. Onsite refers to the place where the system is physically located. First and foremost, the number and type of devices that will be included in the investigation must be identified as well as the documentation of the types and volume of media, including removable media and offsite storage areas and/or remote computing locations. Identification of the proprietary software and the operating system of the device is crucial to the investigation. There is a possibility that these devices are always not connected to any kind of network at some point, so the determination of the existence of a network on-site is needed. With a view to being aware of the level of the system administrators and users, the investigator will interview them. On a general basis, the investigator will have to evaluate the general conditions of the site.

Processing location assessment

Assessment of the evidence must be put through with a view to determining the proper environment where the examination should take place. The examination will preferably occur in a controlled environment, such as a dedicated forensic work area or laboratory. Although, it is possible that circumstances can lead an examiner to fulfill an onsite examination. The investigator should consider the time they will need onsite to recover all the evidence previously mentioned in the document bordering on the suitability of equipment, resources, media, training, and experience they have to properly carry through the onsite evaluation. Long-term deployment and search should be also

contemplated because of the impact on the business and logistics and staff concerns related.

Legal considerations are present in this phase as well in the identification of the reach of the search authority and possible concerns related to the application to different statutes.

Evidence assessment

As mentioned earlier in the document, there is a prioritization of the evidence in the analysis. This is based on the location where evidence is found and the stability of media to be examined. For instance, volatile data must be the first kind of evidence to be examined. One of the factors that require to be taken into consideration is the need for battery-operated devices to provide continuous electric power. In some cases, it is necessary to evaluate the storage locations for EMI to ensure the evidence is not tarnished by this factor. Evidence could be possibly affected during packaging, transport or storage, hence the establishment of the condition of it is crucial when performing the analysis.

3.1.3 Evidence Acquisition

The main goal of this procedure is to acquire the original (or exact copy) digital evidence in such a way that protects and preserves it. This procedure is required as a result of the inherent properties of digital evidence, which is fragile. By the reason of its fragility, it can be easily forged, damaged or destroyed by cause of improper handling or examination. This step is where data is retrieved from where it is allocated originally. This can also include the request and reception communications data; it is not only referred to data allocated on a disk.

The steps performed in this phase will be decisive for the rest of the investigation because it entails the physical extraction of the digital evidence. Hence, security must be guaranteed at all costs. This security must be guaranteed in the examiner's systems as well, both hardware and software configurations and functioning are determining when the investigation is carried through. It is mandatory for the examiner's storage device to be forensically clean when the acquisition of the evidence.

It is possible that the storage devices require physical access by disassembling them to be protected from any external interference. The examiner will determine which devices need to be gathered. Such devices can either be internal, external, or both. All the specifications of the suspect's system need to be listed since it could affect the analysis. Among them, there are the condition of the drive (e.g., make, model, geometry, size, jumper settings, location, drive interface) and internal components (e.g., sound card; video card; network card, including media access control (MAC) address; personal computer memory card international association (PCMCIA) cards).

Despite in some cases, there is a need for battery-operated devices to be continuously provided with electric power, the disconnection of the storage devices to prevent plausible digital evidence to be destructed, damaged or altered is needed depending on the device and the nature of the evidence.

Retrieval of information about the configuration of the suspect's system through several controlled boots. The first one is needed in pursuance of capturing CMOS/BIOS information and test functionality. The second boot is required to test the computer's functionality and the forensic boot disk. And the third one is performed in order to capture the drive configuration information from the CMOS/BIOS.

After all these tasks are performed, the system must be powered down and proceed with the actual acquisition of the storage device using the examiner's system. It is important to configure the device, so it is recognized by the examiner's system.

There are exceptions to the removal of storage devices from certain devices. For RAID (Redundant Array of Inexpensive Disks) its removal may result in not usable results. In laptop systems removal could be inaccessible and if possible, may result in unusable results. In the case of legacy devices there is a hardware dependency, older drives may not be readable in newer systems. There could be also a lack of access to equipment due to unavailability.

Additionally, there are some aspects to consider when treating the data during acquisition. It is advisable to perform an image of the suspected devices instead of working with the original exhibit in order to prevent altering it. When making a copy of the digital evidence, the bit-stream copy option will provide a bit-by-bit image of the original evidence. This will be helpful for the consideration of the copy evidence as to the original for the purpose of investigation. In order to guarantee evidence remains unaltered during the investigation process, the examiner can calculate the checksum or a hash value of both the original evidence and copy. This can also be applied to images.

3.1.4 Evidence Examination

In this step examination on data acquired occurs by the utilization of accepted forensics procedures. This examination will preferably not be conducted on the original evidence.

Preparation

Working directories with evidentiary files and data must be prepared. From these directories, the information should be recovered and/or extracted.

Extraction

There are two types of possible extractions, physical or logical. When the extraction is physical, the data is identified and recovered across the entire physical drive without regard to the file system. If the extraction is logical, files and data are identified and recovered based on the installed operating system, file system and/or applications.

Physical extraction In this stage, several methods can be applied such as keyword searching, file carving and extraction of the partition table and unused space on the physical drive.

Logical extraction In this stage, several methods can be applied such as the extraction of the file system information, data reduction to identify and eliminate known files,

extraction of files pertinent to the examination, recovery of deleted files, extraction password-protected, encrypted and compressed data, extraction of file stack and extraction of the unallocated space.

Analysis of extracted data

Analysis refers to the process of interpreting the data that was previously extracted in views of establishing its significance to the case. The analysis may include these steps:

Timeframe analysis This step can help conclude when events occurred on a system, with this is possible to determine a relationship between usage of the computer and the user at the time the events befell. This analysis also incorporates time and date stamps in the file system metadata "(e.g., last modified, last accessed, created, change of status)" to connect files of interest to relevant time frames. Furthermore, a review of the system and application logs should be considered. Among these logs, it is feasible to encounter error logs, in installation logs, connection logs, security logs, etc.

Data hiding analysis This step is vital considering data can be hidden in the system. This may help with the detection and recovery of data that might indicate knowledge, ownership, or intent. For example, there are methods to intentionally hide data on a system and purposely changing file extensions is one of them. If there are mismatches after performing a correlation between file headers to the corresponding file extensions, this may indicate intentionally hidden data.

Obtaining access to all the files, including password-protected, encrypted, and compressed files is key so as to know if there is an endeavor of concealing the data from unauthorized users.

Further to this, the usage of steganography is another way to hide data. According to the definition found in (Neijts, et al., 2018), “steganography is a technique that hides secret data within an ordinary, non-secret, file or message in order to avoid detection. Later, at its destination, the secret data is extracted.” There are no boundaries when it regards to the type of content that carries the secret data, this includes text, image, video or audio content and many more. Ultimately, the obtention of access to the host-protected area (HPA) is relevant. An effort to conceal data may be suggested by the inclusion of user-generated data in an HPA.

Application and file analysis Programs and files may contain information pertinent for the investigation and supply with awareness about the capability of the system and the knowledge of the user. Amid the methods that can be applied the examiner has to perform the review of file names in search of relevance and patterns, examine of the content of the files, identify of the number and type of operating system, establish a correlation between files and installed applications and relationships between different files, identify of unknown file types to determine their value to the investigation, examine of the file structure of the drive and the users' default storage location for applications [3], examine the user’s configuration settings and analyze of file metadata.

[3] This is performed to determine if files have been stored in their default or an alternate location.

Ownership and possession Throughout the analysis, it is relevant to identify the user that created, modified or accessed a certain file. It may also be critical to determine ownership and knowledgeable possession of the questioned data.

Conclusion

Information derived from each of these steps itself cannot be enough to draw a conclusion. Nonetheless, when considered as a whole, comparisons between the different results may offer a bigger picture of the case. The examiner must consider the results of the extraction and analysis in their entirety.

3.1.5 Documenting and Reporting

This step must be done contemporaneously with the examination, as the actions taken during the digital evidence investigation must be correctly registered. Documentation is an ongoing process throughout the examination. The documentation executed by the examiner must be complete, accurate and comprehensive so interpreters of this information can understand the case correctly. The report may include the identity of the reporting agency, case identifier or submission number, case investigator, the identity of the submitter, date of receipt, date of report, descriptive list of items submitted for examination, (including serial number, make, and model), identity and signature of the examiner, brief description of steps taken during the examination, such as string searches, graphics image searches, and recovering erased files and results/conclusions.

Summary of findings

This section of the report consists of a summary of the results of the examination executed on the system.

Details of findings

This section of the report consists in a deeper description about the results of the examination and it may include specific files related to the request, other files, including deleted files, that support the findings, string searches, keyword searches, and text string searches, internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity, graphic image analysis, indicators of ownership, which could include program registration data, data analysis, description of relevant programs on the examined items and techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies

Supporting materials

List of supporting materials used throughout the examination, such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation.

Glossary

The document can include a glossary to help the reader understand technical terminology.

3.2 Methods

In the previous section on the thesis, the phases of the Digital Forensics Analysis are explained. It is important to note that within these phases, different standard methods can be applied in order to carry out said analysis:

3.2.1 RFC 3227

"*Guidelines for Evidence Collection and Archiving*": All the information included in this section is extracted from the RFC 3227 IETF's website (Brezinski & Killalea, 2002). Description of the procedure taken in the analysis is described in the document of the RFC 3227 in the "Appendices" chapter.

3.2.2 ISO/IEC 27037:2012

Figure 4 illustrates the application of ISO/IEC documents to different phases of the investigation.

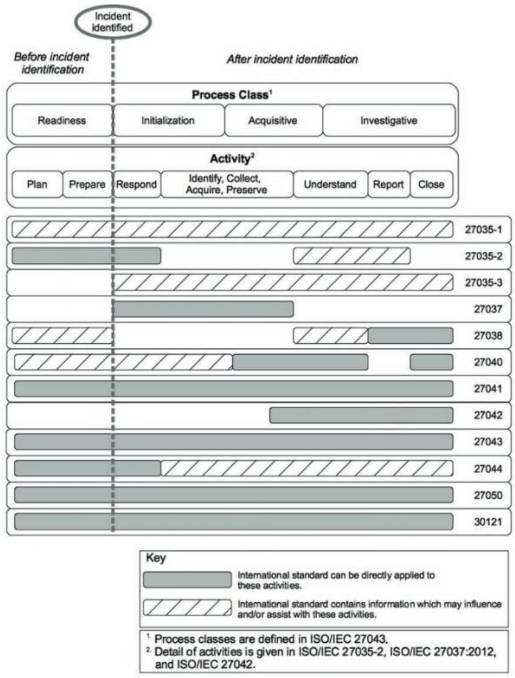


Figure 4. Application of different ISO/IEC standards in the phases of a digital forensics investigation

"*Techniques of Digital Forensics Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*" (ISO/IEC, 2012)

This International Standard provides guidelines for specific activities in handling digital evidence, which are identification, collection, acquisition and preservation of digital evidence that may be of evidential value.

The examiner that is in charge of handling digital evidence should be able to be aware of the potential risks that they can encounter when working with the material. With this International Standard, there is an intention to provide guidance to carry out the investigation properly. This guidance is aimed at the following individuals:

- Digital Evidence First Responders (DEFRs)
- Digital Evidence Specialists (DESs)
- Incident Response Specialists
- Forensic Laboratory Managers

The individuals mentioned above must follow certain principles in order to carry through the investigation correctly (Veber & Smunty, 2015):

- Minimal manipulation with digital devices or digital data.
- Documentation of actions and changes occurred to the digital evidence. Necessary to inform decision-makers who need to determine the reliability of digital evidence presented to them.
- Accordance between the laws of the country.
- DEFR should not act beyond their competence.

This International Standard guides individuals concerning common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions. This International Standard gives guidance for the following devices and/or functions that are used in various circumstances:

Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto-optical disks, data devices with similar functions.

Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards.

- Mobile navigation systems.
- Digital still and video cameras (including CCTV).
- Standard computer with network connections.
- Networks based on TCP/IP and other digital protocols.
- Devices with similar functions as above.

One of the most important points in an investigation is to ensure the integrity and authenticity of the potential digital evidence, because of this reason it will be necessary to carry out an acceptable methodology. However, the International Standard does not mandate the use of particular tools or methods. This will also apply for methodologies for the legal proceedings, disciplinary procedures and other related actions in handling potential digital evidence that are outside the scope of identification, collection, acquisition and preservation.

National laws, rules and regulations must work hand in hand with the International Standard, it will not replace specific legal requirements of any jurisdiction.

3.2.3 ISO/IEC 27041:2015

"Guidance on assuring suitability and adequacy of incident investigative method" (ISO/IEC, 2015)

It offers guidelines on measures to ensure that the procedures and approaches used to evaluate cybersecurity incidents are sufficient. This takes into account whether third-party manufacturers and checks will aid with this assurance process. Its objectives are the following:

Provide directions on the capture and subsequent analysis of both functional and non-functional requirements related to security in incident investigation.

- Using validation to ensure the adequacy of the investigative processes.
- Determine new validation rates and required tests from a validity exercise.
- Select specific evaluations and documentation in the validation process.

This International Standard may be useful to guarantee the validity of digital evidence in court proceedings. It defines part of a comprehensive analysis process that does not only include the following subject areas but also includes:

- Incident management.
- Digital evidence handling.
- IDS and IPS systems, including information that can be obtained from these systems.
- Storage security, including sanitization of storage.
- Ensure the analysis techniques are suitable for purposes.
- Analysis and interpretation of digital evidence.
- Understanding digital evidence forensic concepts and procedures.
- Security incident event management.
- Relationship between electronic discovery and other investigative methods, as well as the use of electronic discovery techniques in other investigations.
- Governance of investigations, including forensic investigations.

3.2.4 ISO/IEC 27042:2015

"Guidelines for the analysis and interpretation of digital evidence" (ISO/IEC, 2015)

This International Standard offers a guide to digital evidence analysis and interpretation. It includes guidance about how the possible digital evidence of an event should be evaluated and viewed to decide and examine which can be needed to justify its comprehension.

It provides a standard context for assessing and evaluating security management incidents and can be used to incorporate new approaches. This also offers a variety of concepts that are relevant to modern digital forensic analysis taking into account that the

usage of a certain method can influence the interpretation of the digital evidence used in the process.

It deals with the analytical models that can be used by digital forensics experts in static or active systems and the considerations to be taken into account in each case, especially attention to incidents in live or active systems such as mobile devices, encrypted systems, networks, etc.

There are two methods to approach live analysis. It is important to consider those systems that cannot be copied and extracted as an image. With this sort of system, there is a risk of losing digital evidence when copied so it will be crucial to try to minimize possible evidence garnishment and ensure there is a complete register of the processes carried out. On the other hand, when there is a possibility to copy or image a system, it will be necessary to interact with it as well as observe its functioning. Other considerations include being careful to emulate the hardware or software of the original environment, using verified virtual machines, copies of the original hardware in order to allow analysis as close as possible to the real one.

Nevertheless, the content of the analysis results in the expert report and its legal considerations are detailed. Finally, it includes the competences of forensic experts: training, learning, skills, objectivity and professional ethics. (ISO/IEC, 2015)

3.2.5 ISO/IEC 27043:2015

"Incident investigation principles and processes" (ISO/IEC, 2015)

Provides guiding principles for incident investigation processes involving digital evidence. It includes the preparation processes prior to the incident through the closure of the investigation, as well as warnings about it. The International Standard describes the processes and principles applicable to the different types of criminal investigations, such as security breaches, system failures, unauthorized access, among many others. It does not offer specific details for each type of investigation, but an overview. of the applicable research principles and processes. (ISO/IEC, 2015)

3.2.6 ISO/IEC 27050

"Information technology— Electronic discovery"

ISO/IEC 27050-1:2019 *Overview and concepts* (ISO/IEC, 2019)

This International Standard is essential as it gives the expert an overview of the term electronic discovery, which "is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding". In this overview terminology, concepts, and processes that are intended to be exploited by other parts of the 27050 series are included. Among the concepts, identification, preservation, collection, processing, review, analysis, and production of ESI are detailed. Electronic discovery turns out to be the unifying thread in

investigations as well as in acquisition and management tasks of the evidence, which can have characteristics such as high sensitivity making special protections required.

ISO/IEC 27050-2:2018 ***Guidance for governance and management of electronic discovery*** (ISO/IEC, 2018)

Organizations, as well as stakeholders within and outside those organizations, at collective and individual risk, may be exposed by participating in electronic discoveries and processes at the legal, financial and ethical levels. This International Standard is intended to guide decision-makers and ensure that compliance and policy requirements continue to be met to enable effective and appropriate electronic discovery and processes.

This document is intended to address the concerns of electronic discovery by identifying risk and risk owners. The purpose of this document is to provide a guide for the governance and management of electronic discovery.

ISO/IEC 27050-3:2020 ***Code of practice for electronic discovery*** (ISO/IEC, 2020)

This International Standard provides requirements and recommendations addressed to both technical and non-technical personnel involved in activities related to electronic discovery. It is important to note that the user is expected to be aware of any applicable jurisdictional requirements. Moreover, additional material is included in order to help organizations have a better understanding of the goals that arise with electronic discovery processes. This document gathers aspects of both 27050-1: 2019 and 27050-2: 2018 to establish a broad framework to specify relevant measures for the reduction of the ESI life span.

4 TOOLS FOR DIGITAL FORENSICS ANALYSIS

Nowadays, there are numerous tools for the digital forensics analysis that can be used for different types of data in a device. Depending on the analysis carried out and the evidence found the tools chosen by the examiner will differ. Among the target of these tools hard drives, storage devices, network topologies, software, mobile phones, laptops are found.

It is important to note that when evidence collection occurs it is better to use portable tools that can be run with USB devices and DVDs, which are executed externally, in order to avoid any kind of corruption in the digital evidence when installing these software applications in the suspect's system.

Subsequently, evidence that is collected and guarded is analyzed in what is called a "Forensics Laboratory". In this lab different hardware and software forensics tools can be used conducive to obtain and analyzed the extracted evidence.

When choosing a tool in the first place the examiner can encounter a huge difficulty due to the repeated problems of reliability, security and support, between the two existing currents: Tools with a commercial purpose which normally keep the procedures hidden for the users and must be paid in order to be used and tools created by a group or organization that are designed as open-source tools. Secondly, there is a problem surrounding the minimum requirements that must be met so that their use on the evidence does no more harm than good.

To guarantee the correct operation and reliability of forensic informatics tools, there are organizations that test and validate them, such as the National Institute of Standards and Technology (NIST) within their Computer Forensics Tool Testing Program (CFTT). The objective of this organization is to establish a methodology for the equipment, criteria and test procedures that allow the development of the tool specifications. The results provide the information necessary for manufacturers to improve their tools, and for users to have sufficient information to decide which software to purchase to obtain accurate and objective results.

In the following tables, from

Table 6 to Table 30 (in "Appendices" chapter), software specified NIST's website are listed (The National Institute of Standards and Technology, 2019). It is essential to note that the majority of these products are commercial solutions. Later in the thesis, software tools available in the market that are not included in NIST's catalog, mostly open source and freeware, are listed and classified.

4.1 Autopsy

Autopsy (The Sleuth Kit, n.d.) is the software computer that represents the graphical interface to the command line digital investigation analysis tools in The Sleuth Kit and it was originally developed by Brian Carrier. These two can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).

The software is maintained by Basis Technology Corp. with the assistance of programmers from the community. The company, as it shows on their website (https://www.autopsy.com/support/training/), offers different support services and training. A very important trait about Sleuth Kit and Autopsy is that both are Open Source and run on UNIX (Linux, Mac OS X, Open & FreeBSD, Solaris, Cygwin) and Windows platforms. Although, different versions are distributed under different licenses. While Autopsy 2 source code is distributed under a GPL 2 license, Autopsy 3 and 4 source code are distributed under a Apache 2 license. It is necessary to point out that the programming languages used for both source codes are different as well, while the version 2 is written in Perl, the version 3 is written in Java using the Netbeans platform.

Autopsy provides certain characteristics that help examiners carry through a more in-depth analysis (WikiPedia, 2020):

- **Extensible:** Through developing plugins, the user should be able to add new functionalities. These plugins can analyze all or part of the underlying data source. Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third parties. (e.g. Timeline Analysis, Hash Filtering, Keyword Search, Web Artifacts, Data Carving, Multimedia, Indicators of Compromise.)
- **Centralized:** A standard process for accessing all functions and modules must be given by the tool.
- **Intuitive:** The browser must allow users to repeat steps taken previously without having to reconfigure excessively by offering wizards and historical tools. It should be noted that digital forensic tools could also be used by non-technical investigators. A proof of this is the Autopsy's default view, which is a simple interface where all the analysis results can always be found in a single tree.
- **Multiple Users:** The tool must hand over the possibility to be usable by a single examiner or a whole team of examiners.
- **Fast:** This is obtained thanks to the execution of several background tasks in parallel using multiple cores. Additionally, certain configurations can be applied in order to obtain a faster speed in analysis such as skipping searching for orphan FAT files and skip analysis of unallocated space and prioritization of user folders and files over system folders and files.
- **Cost Effective:** The software is completely free and at the same time offers the same core features as other digital forensics tools and offers other essential features, such as web artifact analysis and registry analysis, that other commercial tools do not provide.

Additionally, add-one modules [4] can be added to extend the original software package.

[4] Found in https://www.autopsy.com/add-on-modules/

4.2 PhotoRec

PhotoRec is a free and open-source tool that is used for data recovery based on signatures, it recovers various data types including video, documents and archives from hard disks, CD-ROMs, memory cards (CompactFlash, Memory Stick, Secure Digital/SD, Smart Media, Microdrive, MMC, etc.), USB memory drives, DD raw image, EnCase E01 image, etc. This tool is distributed under the GNU General Public License v2 or later. This means the user can run the program for any purpose, read and change the code in order to obtain a certain outcome, redistribute copies and distribute copies of the modified versions to others under the same license.

In order to understand how PhotoRec work, it is important to understand how file systems store files. FAT, NTFS, ext2/ext3/ext4 file systems store them in data blocks 2. The size of these blocks is a constant number of sectors. Generally, operating systems continuously store data with a view of minimizing fragmentation.

Once a file is deleted, metadata about it is lost. This metadata includes file name, date/time, size, location of the first data block/cluster, etc. The first item PhotoRec is going to try to find is the data block size. When an examiner needs to recover deleted files and the file system is not corrupted, it is necessary to take into account how the file systems behave when it comes to deleted data. Although PhotoRec is file system agnostic, meaning it only goes after the underlying data, the software needs to be aware of where the data can be potentially found. In the case of ext2/ext3/ext4, the value for the data block can be read from the superblock. On the other hand, for FAT and NTFS systems, this value can be read from the volume boot record. Else ways, PhotoRec will require to read the media, sector by sector, directed towards finding the block size. Once the value is known by the software, the reading process will be performed block by block. After the blocks are read, these are checked against a signature database that comes with the program.

After the file is recovered, PhotoRec stops its recovery to later check the consistency of the file when feasible and starts to save the new file. The size of this new file will depend on fragmentation. If the data is not fragmented, the size of the new file will be identical or larger than the original. PhotoRec is able to know the original size by reading it from the file header and truncate it, if necessary, to the proper size. If the size of the new file is smaller than the one specified in the header, it ends up being discarded.

When the recovery process is finished, PhotoRec checks the previous data blocks to see if a file signature was found but the file was not able to be successfully recovered and tries it again. This is how fragmented files can be completely recovered. (CGSecurity, 2019)

Information regarding operating systems, file systems and file formats are included in tables in the "Appendices" chapter.

4.3 FTK Imager

FTK Imager is a data preview and imaging tool that is used in order to acquire digital evidence without altering it. These perfect copies are known as forensic images. In or-

der to prevent any manipulation to the evidence, intentional or accidental, the software performs a bit-for-bit duplicate image of the media. By doing so, the forensic image is identical in every way to the original, including file slack and unallocated space or drive free space. After the acquisition is performed, further analysis can be carried through with other forensic tools, for instance, Access Data Forensic Toolkit (FTK). Needless to say, these two tools developed by the AccessData Group, Inc are complementary. As mentioned previously in the thesis, the creation of the image should be one of the first steps taken by an Incident Responder. This is performed with the view of not losing any artifact or evidence about the potential attack. It is also important to note that the software calculates MD5 hash values and confirms the integrity of the data before closing the files.

There are two versions of the software. Installed or portable, the first one runs the full installation on the required system while the second one can be run through a USB stick. (Access Data Group, Inc., 2016).

Information regarding operating systems and file systems are included in tables in the "Appendices" chapter.

4.4 The Volatility Framework

Volatility is a framework used to carry out digital forensics analysis designed by forensics, incident response, and malware experts. It allows a forensics investigator to analyze RAM dumps from 32/64-bit Windows, Linux, Mac and Android systems. It is written in Python, which an established forensic and reverse engineering language with loads of libraries that can easily be integrated with the framework. Volatility is packaged in various formats, including the source code in zip or tar file (for all platforms), a PyInstaller executable (Windows only), and a standalone executable (Windows only).

It is an open-source tool distributed under the GPLv2 license, meaning that the user has the possibility to read, learn from the code and extend it. The user also can immediately fix any issues instead of having to wait for any update from the vendors.

Furthermore, an extensible and scriptable API grants the user the freedom to go beyond and innovate. Analysts can add new address spaces, plugins, data structures, and overlays to truly weld the framework to their needs.

Volatility’s modular design allows it to easily support new operating systems and architectures that do not yet exist. All devices are targets of possible attacks or misfortunes and thanks to Volatility’s modularity it can be adapted to any operating system.

With this tool, it is possible to extract information from running processes, open network sockets, network connections, loaded DLLs from each process and cache log sections, process IDs and more. It also has support to extract information from Windows crash dump files and hibernation files among many other data.

Volatility operates fast and efficient algorithms without unnecessary overhead or memory consumption, this allows RAM dumps of large systems to be analyzed. For starters, in a few seconds volatility will list the kernel modules on an 80 GB system. Although improvements are still necessary, and time varies by command, other memory analysis

frameworks can take much longer to perform the same tasks in much smaller memory dumps. (The Volatility Foundation, 2018)

Information regarding operating systems, file systems and file formats are included in tables in the "Appendices" chapter.

4.5 Advanced Digital Forensics Workstations

The digital forensics workstations must be powerful and high-performance servers that would allow the investigator to conduct the analysis smoothly, this requires a large storage capacity for disk imaging, cloning and backup copies. Additionally, the processes in order to perform the analysis with certain technologies demand a considerable amount of resources.

4.5.1 Ondata

Ondata is a Spanish company that is in charge of design the Velociraptor forensic workstations. They are designed to solve the need for investigators to have the proper hardware in accordance with the analysis software. Ondata technicians have been able to design the right equipment so that researchers from both companies and the security forces can do their work smoothly and safely. These workstations are meant to cover efficiently all the steps in a digital forensics investigation, from data acquisition until reporting. (Ondata, n.d.)

Velociraptor 3

It is equipped with SSD disks to give maximum speed to the Operating System and with RAM memory from 32GB to 256GB, which will allow the examiner to run multiple applications at the same time. In addition, they incorporate write-blocked ports FireWire, USB 3.0, SATA and eSATA, which facilitates connectivity with the different forensic devices that need to be investigated.

Velociraptor 3 incorporates a liquid cooling system, using refrigerant fluids to extract the heat generated by the equipment components, cooling it as a whole. This type of cooling, in addition to being less noisy than cooling with ventilation, increases the frequency of the processors' clocks, taking the equipment to its maximum performance.

They include software with forensic utilities that will be useful for the development of investigations. Also, to prevent possible data loss due to disk failures, it includes disk status monitoring software, which will issue an alert to the user if any of the forensic station's disks deviate from their operating range. Some of the utilities included in these devices are virtualization software, software to work ISO images, disk status monitoring software, hash calculation software, memory Analysis Tool Suite, timeline Analysis, hash filtered Keyword search, Hex editor and PCAP analysis.

Velociraptor 5

It is equipped with SSD disks to give maximum speed to the Operating System and with RAM memory from 128GB or 256GB, which will allow the examiner to run multiple applications at the same time. In addition, they incorporate write-blocked ports FireWire, USB 3.0, SATA and eSATA, which facilitates connectivity with the different forensic devices that need to be investigated.

As it occurs with the Velociraptor 3, Velociraptor 3 incorporates a liquid cooling system, using refrigerant fluids to extract the heat generated by the equipment components, cooling it as a whole. This type of cooling, in addition to being less noisy than cooling with ventilation, increases the frequency of the processors' clocks, taking the equipment to its maximum performance.

Ondata's Velociraptor devices are the only forensic station that incorporates monitoring software that monitors the status of all the disks connected to the station. The software sends notifications that alert the user if any of the disks installed in the equipment deviate from its range of operation, thus corrective and preventive measures can be taken to help prevent data loss. In addition, it includes software with forensic utilities that will be useful for the development of investigations.

The utilities included are the same as in the Velociraptor 3.

Velociraptor 7

It is equipped with 960GB SSD PCi disks to give maximum speed to the Operating System and with 256GB RAM memory, which will allow the researcher to run multiple applications at the same time. To give greater security to the stored data, it offers 32TB in Raid 5 for evidence storage; and to make the investigation quicker and more agile, it includes 2TB in Raid 0 for temporary and 8TB in Raid 0 for cases.

The station includes the DeepSpar Disk Imager 4 solution, which is a disk imaging device capable of recovering data from unstable hard disks with damaged sectors and can recover information that can be of great value for research. The solution brings the Forensics Add-on plug-in active, which allows using ATA commands to disable the automatic relocation of damaged sectors so that more data can be extracted, deleted or viewed master and user passwords from the disk, access to the hidden DCO area, Preparation of forensic reports at the file level including data such as path, name, size, creation date, number of sectors, corrupt sectors, MD5 hash, among others.

It comes equipped with FireWire, USB 3.0, SATA and eSATA write-locked ports, making it easy to connect to the various forensic devices that need investigation.

Following the same steps as Velociraptor 3 and 5, Velociraptor 7 incorporates a liquid cooling system, using refrigerant fluids to extract the heat generated by the equipment components, cooling it as a whole. This type of cooling, in addition to being less noisy than cooling with ventilation, increases the frequency of the processors' clocks, taking the equipment to its maximum performance.

The utilities included are the same as in the Velociraptor 3 and 5.

Table 2. Comparison between Velociraptor models

Velociraptor 3, 5 and 7 Specifications			
			
	Velociraptor 3	**Velociraptor 5**	**Velociraptor 7**
Processor	Dual Xennon 8C	2 x Dual Xennon 12C	2 x Dual Xennon 18C
RAM	64 GB	128 GB	256 GB
S.O. Disk	SSD 128 GB	SSD 256 GB	SSD PCi 960
Temp. Disk	2 TB	SSD 2 TB	2TB in Raid 0 SSD
Evidence Disk	6 TB	18 TB in Raid 5	32 TB in Raid 5
Cases Disk	6 TB	12 TB in Raid 0	8 TB in Raid 0
Operating System	Windows 10 Pro	Windows 10 Pro	Windows 10 Pro
Raid System	No	Yes	Yes
Write Blocker	Yes	Yes	Yes
Card Reader	Yes	Yes	Yes
DeepSpar	No	No	Yes
HotSwap Bay	Yes	Yes	Yes
Blu-Ray	27"	2 x 27"	3 x 27"
Screen	Yes	Yes	Yes
Keyboard	Yes	Yes	Yes
USB 3.0	Yes	Yes	Yes
HDMI	Yes	Yes	Yes
Gbe	Yes	Yes	Yes
FireWire	Yes	Yes	Yes

4.5.2 ADALID

ADALID is a Colombian company that is specialized in computers assembled specially for digital forensics purposes. These workstations are unique in the world and guarantee data processing speed and integrity in said processes. (ADALID, n.d.)

Zeus

High-performance forensic workstation in terms of processing digital evidence, in accordance with the needs for a high volume of data analysis. It is specially made for forensics laboratories that require high availability of storage space through RAID 0, 1, or 5 arrangements, with an excellent high-temperature dissipation.

Table 3. ADALID Zeus Workstation Specifications

 Figure 5. Zeus workstation	Board Dual Socket GA-7PESH3 LGA2011 **Processor:** Intel® Xeon® E5-2600 V2 LGA 2011 (x2). **Screen:** 27-Inch Full-HD 2ms LED with Webcam and Sound. **RAM:** 64GB DDR3 2400Mhz HyperX Beast (Max 256GB). **Connections:** eSATA, SATA3, FireWire, USB 3.0. **Solid State Hard Drive:** 512GB CSSD-F512GBLX, Array x2 HDD 2TB. **Burner:** BluRay DL, DVD RW, CD RW. High-Performance Power Supply. Latest Generation Chassis. **Dissipation:** by Radiator All-In-One Liquid Cooling. GB GDDR5 DIGI+ VRM technology Graphic Card HD7770- 2GD5 x3DVI x1 HDMI **Write Blockers Kit:** Tableau Ultra Kit II model.

Hades

Advanced forensic workstation in terms of processing digital evidence. Specially made for laboratories that demand high speed for acquisition and data analysis without losing probatory force in the evidence. It offers an excellent dissipation of high temperatures. Plus, interconnection capacity with various advanced data transfer technologies such as Thunderbolt, Wi-Fi 2ways, eSATA, SATA3, Bluetooth 4.0, NFC.

Table 4. ADALID Hades Workstation Specifications

 Figure 6. Hades workstation	Board 97-DELUXE (NFC & WLC) ATX DDR3 2600 LGA 1150 **Processor:** Intel Core i7-4790K (8M Cache, up to 4.40 GHz) New 4th Generation. **Screen:** 27-Inch Full-HD 2ms LED with Webcam and Sound. **RAM:** 32GB DDR3 2400Mhz HyperX Beast. **Connections:** eSATA, SATA3, FireWire, USB 3.0, USB 2.0, Thunderbolt, WiFi 2ways, Bluetooth 4.0, NFC, Wireless Charger. **Solid State Hard Drive:** 512GB CSSD-F512GBLX, x1 HDD 2TB. **Burner:** BluRay DL, DVD RW, CD RW. High-Performance Power Supply. Latest Generation Chassis. **Dissipation:** by Radiator All-In-One Liquid Cooling System One Socket. GB GDDR5 DIGI+ VRM technology Graphic Card HD7770-2GD5 x3DVI x1 HDMI **Write Blockers Kit:** Tableau Ultra Kit II model.

Poseidon

Forensic workstation with the proper balance between power, performance, cost and energy consumption. Specially made for small or new forensic laboratories where the priority is based on the stability in processes with adequate hardware according to current technology. Useful for analysis of digital evidence and to provide training on applicable technical methodology, based on forensic computing principles.

Table 5. ADALID Poseidon Workstation Specifications

 Figure 7. Poseidon workstation	**Board Chipset:** Intel Z87 Express x3 PCI-Express 3.0 ATX DDR3 2600 LGA 1150 **Processor:** Intel Core i7-4790S (8M Cache, 3.2 GHz) New 4th Generation. **Screen:** 27-Inch Full-HD 2ms LED with Webcam and Sound. **RAM:** 32GB DDR3 1600Mhz **Connections:** eSATA, SATA3, FireWire, USB 3.0, USB 2.0. Solid State Hard Drive: 256GB CSSD-F512GBLX, x1 HDD 2TB. **Burner:** BluRay DL, DVD RW, CD RW. High-Performance Power Supply 1050W. Latest Generation Chassis. **Dissipation:** by multiple fans(Top, Front, GPU, Back, HDD). **Write Blockers Kit:** Tableau Ultra Kit II model.

4.6 Portable Hardware Devices for Digital Forensics

4.6.1 Logicube: Forensic Talon Ultimate

Figure 8 provides a picture of the device described in this subsection, Talon Ultimate manufactured by Logicube.

Figure 8. Talon Ultimate Imaging Device

Designed for field or forensic lab use, the Talon Ultimate delivers advanced, high-performance forensic imaging at a budget-friendly price. Featuring a compact footprint, user-friendly navigation and unbeatable imaging speed, the Talon Ultimate continues the proud legacy of previous generations of the TalonQR forensic imaging solutions. Engineered specifically for digital forensic investigators, the Talon Ultimate meets all the forensic imaging, hashing and wiping requirements. (Logicube, 2020)

Features: Features to this product are included in the datasheet added as an appendix later in the thesis.

4.6.2 Tableau Forensic Imager TX1

Figure 9 provides a picture of the device described in this subsection, Forensic Imager TX1 manufactured by Tableau.

Figure 9. Tableau Forensic Imager TX1

The OpenText Tableau Forensic Imager (TX1) OpenText (2020) is an imaging solution that operates as a standalone device that can be used both in the lab and on the field. With this device, it is possible to acquire more data, faster "from more media types without sacrificing ease-of-use or portability."

All the features found in this device, which are going to be described later in the document, can be accessed remotely through a web user interface. The web interface can be visited with the following web browsers: Google Chrome, Mozilla Firefox and Safari. Investigators will be able to manage administration/operation and participate in an investigation from any computer within the same network domain. (OpenText, 2020)

Features: Features to this product are included in the datasheet added as an appendix later in the thesis.

4.6.3 Ditto Forensic FieldStation by CRU

Figure 10 provides a picture of the device described in this subsection, Ditto Forensic FieldStation manufactured by CRU.

Figure 10. Ditto Forensic FieldStation

Ditto Forensic FieldStation is a complete and portable toolkit for creating disk clones and images. Ditto FieldStation can be deployed by non-forensics experts and administered and operated remotely by forensics specialists. Via VPN, the Ditto Field- Station can be configured, administered, and managed via an intuitive web browser interface.

It allows the discovery, preview, and image files from hard drives and network file systems. Going further, physical imaging of complete hard drives it attained and logical imaging of specific file types from hard drives and network file systems. A big advantage of this product is the fact that it is always completely free to keep the device updated as well as a free 3-year warranty and no annual fees. This is an important feature to take into account because of the already high prices of most of the tools required in the Digital Forensics field. (CRU, 2020)

Features: Features to this product are included in the datasheet added as an appendix later in the thesis.

5 CASE STUDY: INSIDER THREAT – DATA LEAK

The practical framework will cover the case of "Business Data Leak". The material used for the development of this practical case is made up of free samples/templates obtained through the Internet from various sites. The data sets used are documents with extensions .doc, .ppt and .xlsx. The analysis of the evidence will be carried out with the Autopsy software previously discussed in the thesis. The reason why the analysis is going to be conducted with this software it is because of its open-source nature and a vast range of utilities. It is the best choice if the election is based on price and quality. In order to be able to understand how to properly use the software in question, it was necessary to take the Training course available on the developer's website without damaging the data evidence.

The data evidence will be extracted from a .vdmk file. So as to create the case a virtual machine was required to perform the malicious actions. This virtual machine runs on Windows 10.

5.1 Description of the case

The development of the case begins with the contact by the CEO of the company Bioerts. The procedure is accepted by the company specialized in DFIR, Cybersecua. In this email, Morgan conveys his concern about a possible data leak from an accounting department employee to a competing company.

5.2 Assessment

5.2.1 Materials

The analysis is carried through in a MacBook Pro 13" Retina early with a 150GB Boot-Camp partition. In the following bullet list, specifications for the system are mentioned:

- **Operating System:** Microsoft Windows 10 Pro Education N
- **Processor:** Intel(R) Core(TM) i5-5257U CPU @ 2.70GHz
- **RAM:** 8GB
- **System type:** 64-bit Operating System, x64-based processor

As for the material to examine, it is extracted from a virtual machine created with VirtualBox. In the following bullet list, specifications for the system are mentioned:

- **Name:** Spooner_Accounting
- **Operating System:** Microsoft Windows 10 Pro for Workstations
- **RAM:** 4 GB
- **System type:** 64-bit Operating System, x64-based processor
- **BaseBoard Product:** VirtualBox 1.2

As for software, the forensics tools used in order to perform the investigation were FTK Imager (version 4.2.0) and Autopsy (version 4.14.0). FTK Imager was used to obtain a disk image to later analyze in Autopsy. The procedure carried through in the examination is explained later in the thesis.

5.2.2 Insider Threat: Definition and Indicators

The definition of Insider Threat includes the threats as anyone that has authorized and legitimate access to certain resources and uses this access to intentionally or unintentionally harm an organization and negatively impact the organization's critical information or systems. Insiders can be employees, vendors, partners, suppliers, etc. and according to Verizon (2019) there are 5 common types of dangerous insiders.

The first group comprises the disgruntled employees, these employees might be dissatisfied with several aspects in the work-field. The main reason can be the rejection in a petition for a promotion or a salary raise and poor relationships with colleagues and/or managers. The aim of this kind of insiders is to harm the organization utilizing the destruction of data or disruption of business activity.

The second group is composed of the malicious insiders, these are workers who exploit or abuse access for the theft, leakage or deletion of important company records. The contrast between these employees and the ones mentioned in the previous paragraph is their motivation. Disgruntled employees are moved by emotional response, while malicious insiders use existing privileges to access information for personal gain.

The third group comprehends the inside agents. Within the business are corporate or government agents that can be recruited, approached or persuaded by external parties to exfiltrate data. A new arriver or a trustworthy employee can be an inside agent. Their goal is to steal the intellectual secrets in return for a benefit for the competitors.

The fourth group contains regular and/or careless employees. These are employees or partners that end up misappropriating assets, breaking permissible usage measures, mismanaging information, installing unauthorized applications and utilizing unauthorized workarounds, are mistaking for malicious measures, most of which fall within the IT Shadow world. They normally possess limited access to sensitive data. They will also, either by accident or become the target of phishing, leak data or damage the business network unintentionally.

The fifth group involves third-party providers and contractors. These are business associates that risk protection through negligence, misuse or malicious access to or use of an asset. Security on sensitive data is not guaranteed in some cases due to little to no control over cybersecurity on the side of third-party providers.

The Potential Indicators of Insider Threat Activity may include:

- Aims or successful access without a valid "need-to-know" to systems and records.
- Requesting access to information apart from regular duties.
- Unusual or erratic behavior.
- Highly disgruntled attitude.

- Working at peculiar or late hours for little to no reason.
- Noticeable Unexplained economic growth or excessive indebtedness.
- Striving to disguise foreign contacts, travel, interests or suspicious activities.
- Unreported offers of financial assistance, gifts or favors by a foreign national.

5.3 Acquisition: Disk Image creation with FTK Imager

This step in the investigation corresponds to the "Evidence Acquisition" phase. It is crucial because it entailed the obtaining of the evidence without altering it or tampering it. In order to create the disk in FTK the following steps are needed:

1. In the File Menu, select the "Create Disk Image" option.
2. A wizard guides the user through the process. The type of source is selected among the different options offered. The user in this case picks the “Image File” type and selects the source path.
3. After the image source is selected, the image destination type must be selected among the options offered in the wizard. The user selects E01 as the destination image type.
4. The investigator must fill the form with the Evidence Item Information in order to always keep track of the case.
5. Finally, the image destination folder must be selected as well as the image filename. In this step is also possible to define the image fragment size, the compression and the use of AD encryption. It is important to keep in mind that source and destination require to be in separated storage units (i.e. different partitions)
6. After the configuration for the imaging process takes place, FTK Imager creates the image. This may take time depending on the configuration the examiner uses and the hardware capabilities of the examiner’s system.
   After the "Creating Image" process is performed, the application outputs the verification information to the user.
   Along with the. E01 file, a text documented is generated in the destination folder. In this thesis, the information about the case and the image is included. It is included in the "Appendices" chapter.

5.4 Examination: Data analysis with Autopsy

The first step when conducting a digital forensics examination would be the creation of a new case.

The next step is the addition of one or more data sources. In this case, the data source will be the image of the disk (format. E01) created with FTK Imager as previously mentioned in this thesis.

As it was explained in the theoretical part of the thesis, the configuration of the Ingest Modules is necessary. These modules are the ones in charge of analyzing the data.

After Autopsy processes the data, the results start appearing in the Tree Viewer on the left side of the user interface. As ingest occurs, more results are available in the Tree. Figure 11 illustrates the Tree Viewer of the case in the software Autopsy.

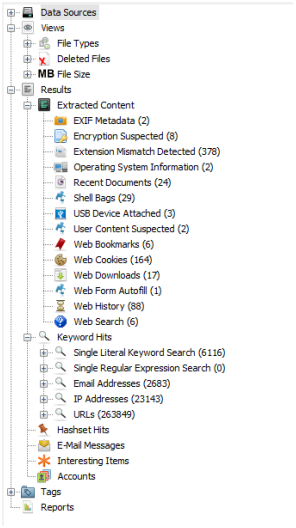


Figure 11. Tree Viewer of the case in Autopsy

The next step encompasses the examination of the different sources of evidence which can be the *Web Search*, *Web History*, *Web Downloads*, *E-mail Messages* and the *Windows Artifacts*.

5.4.1 Web Search

Figure 12 illustrates the web searches performed by the attacker with his system.

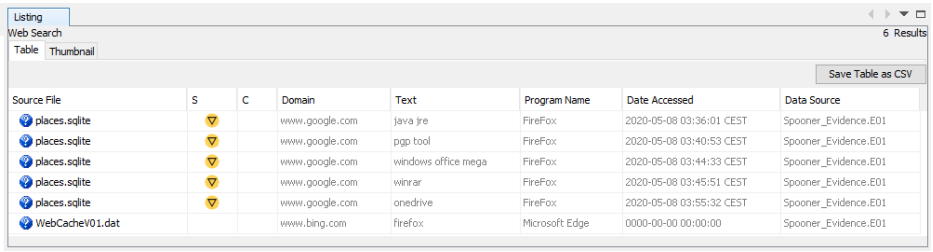


Figure 12. Web Search in Autopsy

5.4.2 Web Downloads

The potentially leaked information was in the suspect's OneDrive shared folder. This information was shared with him by CEO Calvin Morgan. According to Morgan, the reason why the information was stored in that location is so that it was possible to keep a record of the changes made in the documents in addition to having them at any time. It is easy to edit given the Office Online option offered by the platform.

Some guidelines required workers to modify these documents directly from the OneDrive's web application. Therefore, downloading and offline editing of these documents was strictly prohibited. This policy arises from the sensitivity of the information.

Moreover, downloading additional software other than the ones installed on the device at the time of assignment was prohibited. Systems were customized for each employee, so they already had all the necessary programs. Figure 13 illustrates the web downloads performed by the attacker with his system.

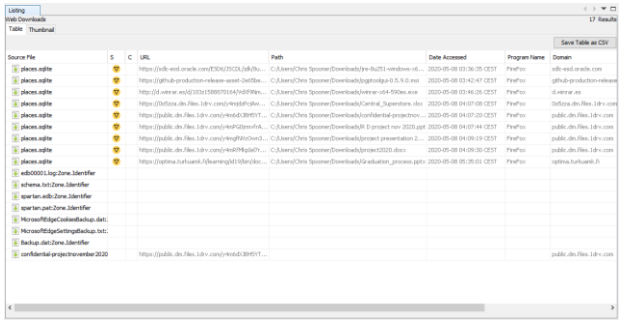


Figure 13. Web Downloads in Autopsy

Besides downloading the files, it was noted that additionally the attacker illegally downloaded a copy of Microsoft Office 2019 as well as an installer for a PGP Tool. The illegal download could potentially infect the system due to the user's lack of skills in the field. By installing the PGP Tool, the no installing new software policy was violated as well.

5.4.3 Web History

There are relevant items in the browser's history such as the following visited pages. Figure 14 illustrates the web history of the attacker's system.

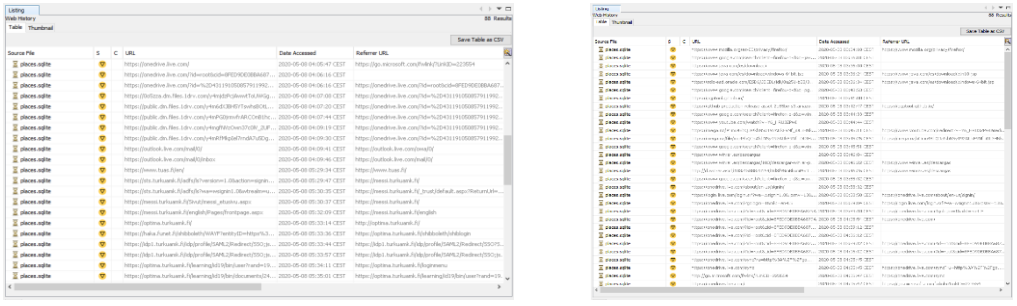


Figure 14. Web History in Autopsy

It is essential to note that for this case study the competitor's website was represented with the URLs for https://www.tuas.fi and https://www.optima.turkuamk.fi. These two websites were used in order to pretend the attacker had access to the competitor's site and other domains of it, such as Optima that required a sign-in. After signing in, the attacker also downloaded a file from the latter website.

5.4.4 Windows Artifacts

Open/Save MRU

This key keeps track of the list of recently opened or saved files via Windows Explorer-style dialog boxes (Open/Save dialog box). This includes web browsers like Internet Explorer or Firefox and a majority of commonly used applications. Figure 15 illustrates the contents of the Open/Save MRU artifact in Autopsy.

Location:

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU`

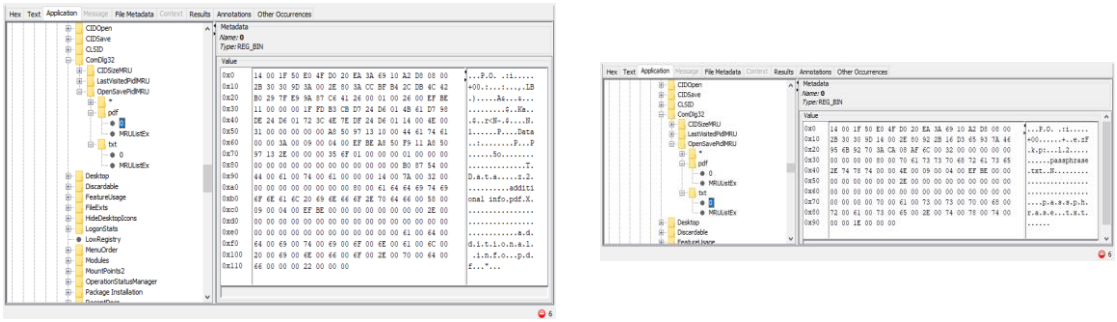


Figure 15. Open/Save MRU Artifact in Autopsy

Windows 10 Timeline

It is a feature that keeps a chronological record of the tasks performed in a PC. It includes the visited websites, edited Office documents and used multimedia files. This data is recorded in a SQLite database. It is very important not to confuse this with the "Timeline" created by different digital forensic tools.

Location:

`C:\Users\<profile>\AppData\Local\ConnectedDevicesPlatform\L.<profile>\ActivitiesCache.db`

This database is composed of the master table, along with seven tables: `'Activity'`, `'Activity_PackageId'`, `'ActivityAssetCache'`, `'ActivityOperation'`, `'AppSettings'`, `'ManualSequence'` and `'Metadata'`.

Each of these tables store information that is relevant to the system. There are three that store information regarding user activities: `'Activity'`, `'ActivityOperation'` and `'Activity_PackageID'`. When there is any new application execution, a new entry to the

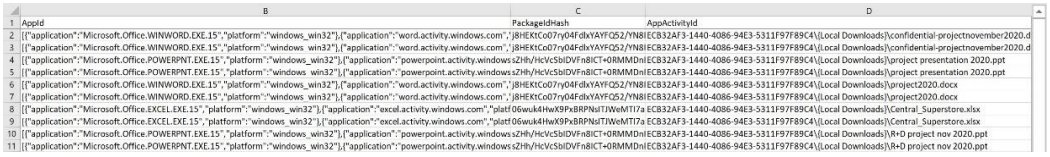
table ’Activity’ is added and subsequently, it results in relevant entries in the ’Activity_PackageID’ table.

It is important to understand the data in these tables in order to know what the user executed in the system. The ’Activity’ table has a unique ID for each entry/user activity, this value can be seen in the table ’Activity_PackageID’ as well. The number of times the ID appears in the second table will depend on the ’Platform’ field. These are the values the examiner needs to check to understand the user’s actions. (Katsavounidis, 2018)

This artifact can be inspected with a browser for SQLite databases. For the sake of this case study, DB Browser (SQLite) was the tool chosen to perform this task. In order to take a better look at the data, the tables were exported as CSV files that could be visualized in Microsoft Excel. Relevant data was found in the tables ’Activity’ and ‘Activity_PackageID’. In both tables was able to determine that the attacker followed these steps:

1. Opened locally the original files downloaded from the OneDrive shared folder.
2. Renamed the files and modified one of the Word documents to add clarifying notes.
3. Encrypted the files with the PGP Tool, which requires Java Runtime Environment 1.8+ to function.
4. Used the Outlook application to send the encrypted files, the keys and the passphrase.

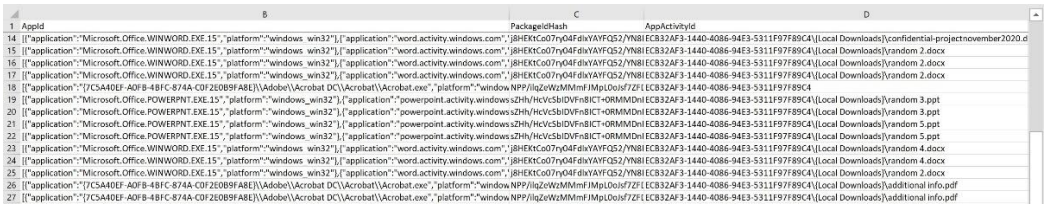
Figure 16 illustrates the actions of opening the downloaded files in Word, PowerPoint and Excel.



	B	C	D
1	AppId	PackageIdHash	AppActivityId
2	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\confidential-projectnovember2020.d	
3	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\confidential-projectnovember2020.d	
4	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows sZHh/HcVcSbIDVFn8ICT+0RMMDnI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\project presentation 2020.ppt	
5	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows sZHh/HcVcSbIDVFn8ICT+0RMMDnI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\project presentation 2020.ppt	
6	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\project2020.docx	
7	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\project2020.docx	
8	[{"application":"Microsoft.Office.EXCEL.EXE.15","platform":"windows_win32"},{"application":"excel.activity.windows.com","platf	06wuk4HwX9PxBRPNsITJWeMTI7a	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\Central_Superstore.xlsx
9	[{"application":"Microsoft.Office.EXCEL.EXE.15","platform":"windows_win32"},{"application":"excel.activity.windows.com","platf	06wuk4HwX9PxBRPNsITJWeMTI7a	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\Central_Superstore.xlsx
10	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows sZHh/HcVcSbIDVFn8ICT+0RMMDnI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\R+D project nov 2020.ppt	
11	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows sZHh/HcVcSbIDVFn8ICT+0RMMDnI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\R+D project nov 2020.ppt	

Figure 16. Table ’Activity’: Opening original downloaded files

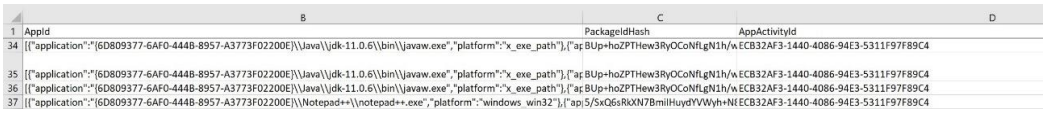
Figure 17 illustrates the actions of opening the renamed files in Word, PowerPoint and Excel as well as modifying the file ‘random’.



	B	C	D
1	AppId	PackageIdHash	AppActivityId
14	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\confidential-projectnovember2020.d	
15	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 2.docx	
16	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 2.docx	
17	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 2.docx	
18	[{"application":"{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Adobe\\Acrobat DC\\Acrobat\\Acrobat.exe","platform":"window	NPP/iIqZeWzMMmFJMpLOoJsf7ZFI	ECB32AF3-1440-4086-94E3-5311F97F89C4
19	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows sZHh/HcVcSbIDVFn8ICT+0RMMDnI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 3.ppt	
20	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows sZHh/HcVcSbIDVFn8ICT+0RMMDnI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 3.ppt	
21	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows sZHh/HcVcSbIDVFn8ICT+0RMMDnI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 5.ppt	
22	[{"application":"Microsoft.Office.POWERPNT.EXE.15","platform":"windows_win32"},{"application":"powerpoint.activity.windows sZHh/HcVcSbIDVFn8ICT+0RMMDnI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 5.ppt	
23	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 4.docx	
24	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 4.docx	
25	[{"application":"Microsoft.Office.WINWORD.EXE.15","platform":"windows_win32"},{"application":"word.activity.windows.com","j8HEKtCo07ry04FdlxYAYFQ52/YN8I	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\random 2.docx	
26	[{"application":"{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Adobe\\Acrobat DC\\Acrobat\\Acrobat.exe","platform":"window	NPP/iIqZeWzMMmFJMpLOoJsf7ZFI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\additional info.pdf
27	[{"application":"{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Adobe\\Acrobat DC\\Acrobat\\Acrobat.exe","platform":"window	NPP/iIqZeWzMMmFJMpLOoJsf7ZFI	ECB32AF3-1440-4086-94E3-5311F97F89C4\{Local Downloads}\additional info.pdf

Figure 17. Table ’Activity’: Opening renamed files and modifying ’random 2’

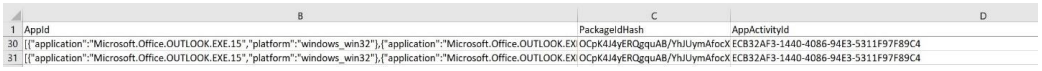
Figure 18 illustrates the usage of the PGP Tool to encrypt the data.



	B	C	D
1	AppId	PackageIdHash	AppActivityId
34	[{"application":"{6D809377-6AF0-444B-8957-A3773F02200E}\\Java\\jdk-11.0.6\\bin\\javaw.exe","platform":"x_exe_path"},{"ap	BUp+hoZPTHew3RyOCoNfLgN1h/w	ECB32AF3-1440-4086-94E3-5311F97F89C4
35	[{"application":"{6D809377-6AF0-444B-8957-A3773F02200E}\\Java\\jdk-11.0.6\\bin\\javaw.exe","platform":"x_exe_path"},{"ap	BUp+hoZPTHew3RyOCoNfLgN1h/w	ECB32AF3-1440-4086-94E3-5311F97F89C4
36	[{"application":"{6D809377-6AF0-444B-8957-A3773F02200E}\\Java\\jdk-11.0.6\\bin\\javaw.exe","platform":"x_exe_path"},{"ap	BUp+hoZPTHew3RyOCoNfLgN1h/w	ECB32AF3-1440-4086-94E3-5311F97F89C4
37	[{"application":"{6D809377-6AF0-444B-8957-A3773F02200E}\\Notepad++\\notepad++.exe","platform":"windows_win32"},{"ap	5/SxQ6sRkXN7BmilHuydYVWyh+N	ECB32AF3-1440-4086-94E3-5311F97F89C4

Figure 18. Table '`Activity`': Encryption with PGP Tool

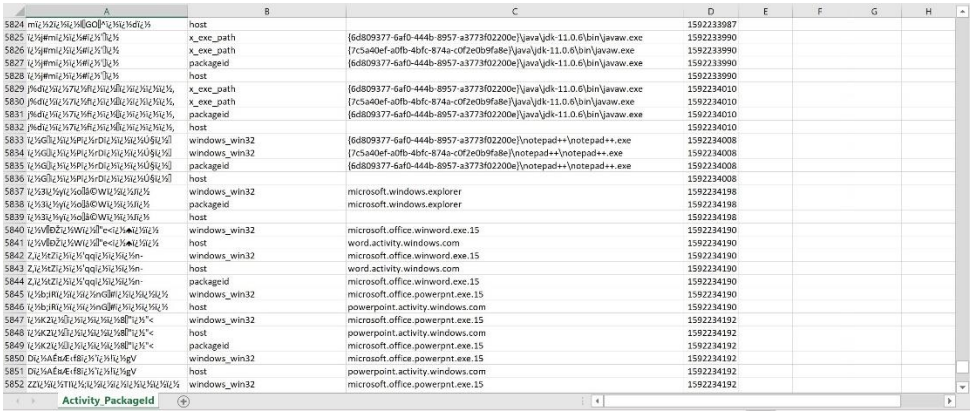
Figure 19 illustrates the usage of the Outlook application to send encrypted data.



	B	C	D
1	AppId	PackageIdHash	AppActivityId
30	[{"application":"Microsoft.Office.OUTLOOK.EXE.15","platform":"windows_win32"},{"application":"Microsoft.Office.OUTLOOK.EX	OCpK4J4yERQgquAB/YhJUymAfocX	ECB32AF3-1440-4086-94E3-5311F97F89C4
31	[{"application":"Microsoft.Office.OUTLOOK.EXE.15","platform":"windows_win32"},{"application":"Microsoft.Office.OUTLOOK.EX	OCpK4J4yERQgquAB/YhJUymAfocX	ECB32AF3-1440-4086-94E3-5311F97F89C4

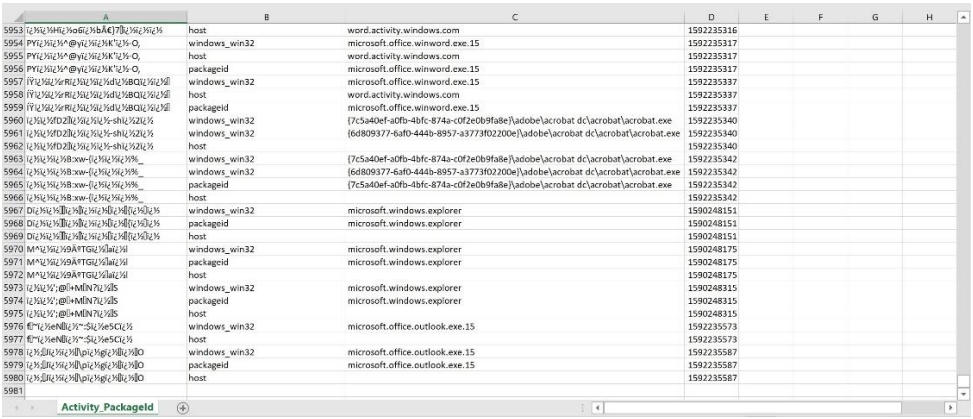
Figure 19. Table '`Activity`': Outlook usage

The same information can be found in the second table mentioned previously. Figure 20 and Figure 21illustrate the same actions previously mentioned.



	A	B	C	D
5824	mï¿½2ï¿½ï¿½[GOÎ[ï¿½ï¿½ï¿½dï¿½	host		1592233987
5825	ï¿½#mï¿½ï¿½#ï¿½'ï¿½	x_exe_path	{6d809377-6af0-444b-8957-a3773f02200e}\java\jdk-11.0.6\bin\javaw.exe	1592233990
5826	ï¿½#mï¿½ï¿½#ï¿½'ï¿½	x_exe_path	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\java\jdk-11.0.6\bin\javaw.exe	1592233990
5827	ï¿½#mï¿½ï¿½#ï¿½'ï¿½	packageid	{6d809377-6af0-444b-8957-a3773f02200e}\java\jdk-11.0.6\bin\javaw.exe	1592233990
5828	ï¿½#mï¿½ï¿½#ï¿½'ï¿½	host		1592233990
5829	ï%dï¿½ï¿½7ï¿½ï¿½#ï¿½Mï¿½ï¿½ï¿½ï¿½,	x_exe_path	{6d809377-6af0-444b-8957-a3773f02200e}\java\jdk-11.0.6\bin\javaw.exe	1592234010
5830	ï%dï¿½ï¿½7ï¿½ï¿½#ï¿½Mï¿½ï¿½ï¿½ï¿½,	x_exe_path	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\java\jdk-11.0.6\bin\javaw.exe	1592234010
5831	ï%dï¿½ï¿½7ï¿½ï¿½#ï¿½Mï¿½ï¿½ï¿½ï¿½,	packageid	{6d809377-6af0-444b-8957-a3773f02200e}\java\jdk-11.0.6\bin\javaw.exe	1592234010
5832	ï%dï¿½ï¿½7ï¿½ï¿½#ï¿½Mï¿½ï¿½ï¿½ï¿½,	host		1592234010
5833	ï¿½Gï¿½ï¿½ï¿½Pï¿½rDï¿½ï¿½ï¿½Ú§ï¿½	windows_win32	{6d809377-6af0-444b-8957-a3773f02200e}\notepad++\notepad++.exe	1592234008
5834	ï¿½Gï¿½ï¿½ï¿½Pï¿½rDï¿½ï¿½ï¿½Ú§ï¿½	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\notepad++\notepad++.exe	1592234008
5835	ï¿½Gï¿½ï¿½ï¿½Pï¿½rDï¿½ï¿½ï¿½Ú§ï¿½	packageid	{6d809377-6af0-444b-8957-a3773f02200e}\notepad++\notepad++.exe	1592234008
5836	ï¿½Gï¿½ï¿½ï¿½Pï¿½rDï¿½ï¿½ï¿½Ú§ï¿½	host		1592234008
5837	ï¿½3ï¿½ï¿½ï¿½olâ©Wï¿½ï¿½ï¿½ï¿½	windows_win32	microsoft.windows.explorer	1592234198
5838	ï¿½3ï¿½ï¿½ï¿½olâ©Wï¿½ï¿½ï¿½ï¿½	packageid	microsoft.windows.explorer	1592234198
5839	ï¿½3ï¿½ï¿½ï¿½olâ©Wï¿½ï¿½ï¿½ï¿½	host		1592234198
5840	ï¿½vÎbŽï¿½ï¿½Wï¿½Îe<ï¿½ï¿½•ï¿½ï¿½	windows_win32	microsoft.office.winword.exe.15	1592234190
5841	ï¿½vÎbŽï¿½ï¿½Wï¿½Îe<ï¿½ï¿½•ï¿½ï¿½	host	word.activity.windows.com	1592234190
5842	Z¸ï¿½tZï¿½ï¿½'qqï¿½ï¿½ï¿½n-	windows_win32	microsoft.office.winword.exe.15	1592234190
5843	Z¸ï¿½tZï¿½ï¿½'qqï¿½ï¿½ï¿½n-	host	word.activity.windows.com	1592234190
5844	Z¸ï¿½tZï¿½ï¿½'qqï¿½ï¿½ï¿½n-	packageid	microsoft.office.winword.exe.15	1592234190
5845	ï¿½bJRï¿½ï¿½ï¿½nGÎRï¿½ï¿½ï¿½ï¿½	windows_win32	microsoft.office.powerpnt.exe.15	1592234190
5846	ï¿½bJRï¿½ï¿½ï¿½nGÎRï¿½ï¿½ï¿½ï¿½	host	powerpoint.activity.windows.com	1592234190
5847	ï¿½ïK2ï¿½Dï¿½ï¿½ï¿½ï¿½ï¿½ÐÎ"ï¿½'<	windows_win32	microsoft.office.powerpnt.exe.15	1592234192
5848	ï¿½ïK2ï¿½Dï¿½ï¿½ï¿½ï¿½ï¿½ÐÎ"ï¿½'<	host	powerpoint.activity.windows.com	1592234192
5849	ï¿½ïK2ï¿½Dï¿½ï¿½ï¿½ï¿½ï¿½ÐÎ"ï¿½'<	packageid	microsoft.office.powerpnt.exe.15	1592234192
5850	Dï¿½AÉ¤Ë·fBï¿½'ï¿½Ï¿½gV	windows_win32	microsoft.office.powerpnt.exe.15	1592234192
5851	Dï¿½AÉ¤Ë·fBï¿½'ï¿½Ï¿½gV	host	powerpoint.activity.windows.com	1592234192
5852	ZZï¿½ï¿½TÏï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½ï¿½	windows_win32	microsoft.office.powerpnt.exe.15	1592234192

Figure 20. Table '`Activity_PackageID`'



	A	B	C	D
5953	ï¿½ï¿½Hï¿½¤oBï¿½bÃ€)7Bï¿½ï¿½ï¿½	host	word.activity.windows.com	1592235316
5954	PYï¿½ï¿½^@yï¿½ï¿½K'ï¿½- O,	windows_win32	microsoft.office.winword.exe.15	1592235317
5955	PYï¿½ï¿½^@yï¿½ï¿½K'ï¿½- O,	host	word.activity.windows.com	1592235317
5956	PYï¿½ï¿½^@yï¿½ï¿½K'ï¿½- O,	packageid	microsoft.office.winword.exe.15	1592235317
5957	ïYï¿½ï¿½rRï¿½ï¿½ï¿½dï¿½BCIï¿½ï¿½Ð	windows_win32	microsoft.office.winword.exe.15	1592235337
5958	ïYï¿½ï¿½rRï¿½ï¿½ï¿½dï¿½BCIï¿½ï¿½Ð	host	word.activity.windows.com	1592235337
5959	ïYï¿½ï¿½rRï¿½ï¿½ï¿½dï¿½BCIï¿½ï¿½Ð	packageid	microsoft.office.winword.exe.15	1592235337
5960	ï¿½ï¿½fD2Bï¿½ï¿½ï¿½Y-shï¿½ï¿½ï¿½	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235340
5961	ï¿½ï¿½fD2Bï¿½ï¿½ï¿½Y-shï¿½ï¿½ï¿½	windows_win32	{6d809377-6af0-444b-8957-a3773f02200e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235340
5962	ï¿½ï¿½fD2Bï¿½ï¿½ï¿½Y-shï¿½ï¿½ï¿½	host		1592235340
5963	ï¿½ï¿½ï¿½B:xw-{ï¿½ï¿½ï¿½%_	windows_win32	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235342
5964	ï¿½ï¿½ï¿½B:xw-{ï¿½ï¿½ï¿½%_	windows_win32	{6d809377-6af0-444b-8957-a3773f02200e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235342
5965	ï¿½ï¿½ï¿½B:xw-{ï¿½ï¿½ï¿½%_	packageid	{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}\adobe\acrobat dc\acrobat\acrobat.exe	1592235342
5966	ï¿½ï¿½ï¿½B:xw-{ï¿½ï¿½ï¿½%_	host		1592235342
5967	Dï¿½ï¿½ï¿½Bï¿½ï¿½ï¿½Bï¿½ï¿½ï¿½	windows_win32	microsoft.windows.explorer	1590248151
5968	Dï¿½ï¿½ï¿½Bï¿½ï¿½ï¿½Bï¿½ï¿½ï¿½	packageid	microsoft.windows.explorer	1590248151
5969	Dï¿½ï¿½ï¿½Bï¿½ï¿½ï¿½Bï¿½ï¿½ï¿½	host		1590248151
5970	M^ï¿½ï¿½9Aï¿½TGï¿½ï¿½aï¿½ï¿½	windows_win32	microsoft.windows.explorer	1590248175
5971	M^ï¿½ï¿½9Aï¿½TGï¿½ï¿½aï¿½ï¿½	packageid	microsoft.windows.explorer	1590248175
5972	M^ï¿½ï¿½9Aï¿½TGï¿½ï¿½aï¿½ï¿½	host		1590248175
5973	ï¿½ï¿½';@ï¿½MÎN7ï¿½ï¿½	windows_win32	microsoft.windows.explorer	1590248315
5974	ï¿½ï¿½';@ï¿½MÎN7ï¿½ï¿½	packageid	microsoft.windows.explorer	1590248315
5975	ï¿½ï¿½';@ï¿½MÎN7ï¿½ï¿½	host		1590248315
5976	¶"ï¿½eNBï¿½'':Šï¿½e5Cï¿½	windows_win32	microsoft.office.outlook.exe.15	1592235573
5977	¶"ï¿½eNBï¿½'':Šï¿½e5Cï¿½	host		1592235573
5978	ï¿½Bï¿½ï¿½ï¿½Bï¿½pï¿½gï¿½Bï¿½O	windows_win32	microsoft.office.outlook.exe.15	1592235587
5979	ï¿½Bï¿½ï¿½ï¿½Bï¿½pï¿½gï¿½Bï¿½O	packageid	microsoft.office.outlook.exe.15	1592235587
5980	ï¿½Bï¿½ï¿½ï¿½Bï¿½pï¿½gï¿½Bï¿½O	host		1592235587
5981				

Figure 21. Table '`Activity_PackageID`'

Last-Visited MRU

Works in tune with the OpenSaveMRU key by tracking the executable used to open the listed files in the previously mentioned key. Moreover, the directory that contains the last file that was accessed in tracked as well. Figure 22 illustrates the contents of the Last-Visited MRU artifact in Autopsy.

Location:

`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPIDlMRU`

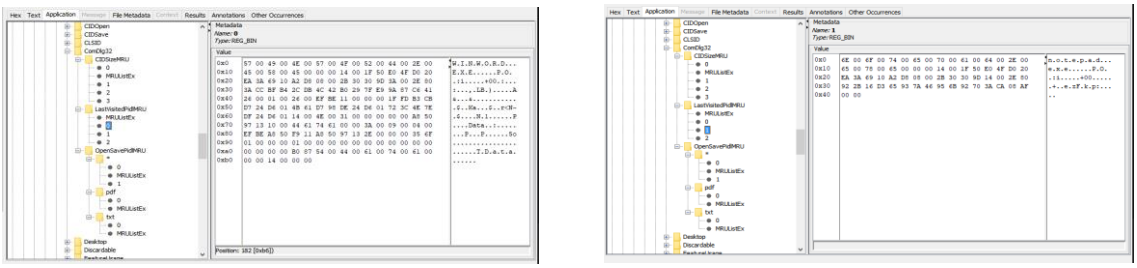


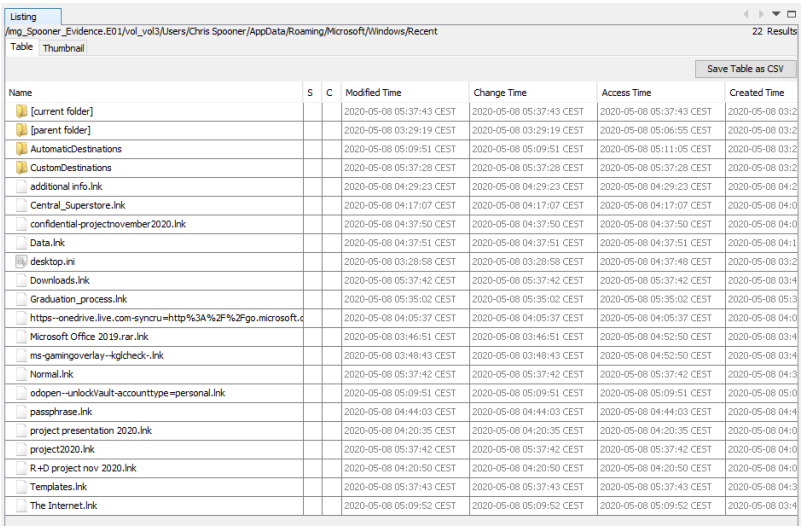
Figure 22. Last-Visited MRU Artifact in Autopsy

Shortcut (LNK) Files

These are shortcut files that are automatically created by Windows. It works as a pointing reference to a file, application or directory. They are generated when opening local or remote files and documents. Figure 23 illustrates the list of LNK files in Autopsy. While Figure 24 illustrates the list of LNK files in the investigator's system.

Primary Locations:

`C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\`
`C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\`

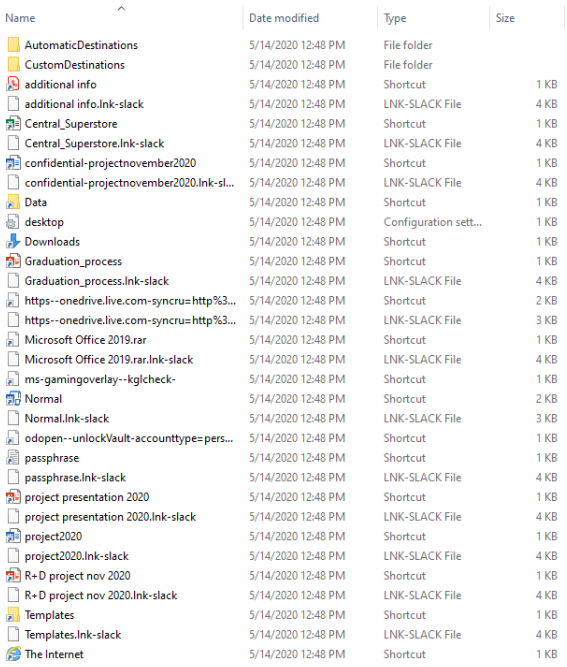


Listing
/img_Spooner_Evidence.E01/vol_vol3/Users/Chris Spooner/AppData/Roaming/Microsoft/Windows/Recent — 22 Results

Table | Thumbnail — Save Table as CSV

Name	S	C	Modified Time	Change Time	Access Time	Created Time
[current folder]			2020-05-08 05:37:43 CEST	2020-05-08 05:37:43 CEST	2020-05-08 05:37:43 CEST	2020-05-08 03:2
[parent folder]			2020-05-08 03:29:19 CEST	2020-05-08 03:29:19 CEST	2020-05-08 05:06:55 CEST	2020-05-08 03:2
AutomaticDestinations			2020-05-08 05:09:51 CEST	2020-05-08 05:09:51 CEST	2020-05-08 05:11:05 CEST	2020-05-08 03:2
CustomDestinations			2020-05-08 05:37:28 CEST	2020-05-08 05:37:28 CEST	2020-05-08 05:37:28 CEST	2020-05-08 03:2
additional info.lnk			2020-05-08 04:29:23 CEST	2020-05-08 04:29:23 CEST	2020-05-08 04:29:23 CEST	2020-05-08 04:2
Central_Superstore.lnk			2020-05-08 04:17:07 CEST	2020-05-08 04:17:07 CEST	2020-05-08 04:17:07 CEST	2020-05-08 04:0
confidential-projectnovember2020.lnk			2020-05-08 04:37:50 CEST	2020-05-08 04:37:50 CEST	2020-05-08 04:37:50 CEST	2020-05-08 04:0
Data.lnk			2020-05-08 04:37:51 CEST	2020-05-08 04:37:51 CEST	2020-05-08 04:37:51 CEST	2020-05-08 04:1
desktop.ini			2020-05-08 03:28:58 CEST	2020-05-08 03:28:58 CEST	2020-05-08 04:37:48 CEST	2020-05-08 03:2
Downloads.lnk			2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 03:4
Graduation_process.lnk			2020-05-08 05:35:02 CEST	2020-05-08 05:35:02 CEST	2020-05-08 05:35:02 CEST	2020-05-08 05:3
https--onedrive.live.com-syncru=http%3A%2F%2Fgo.microsoft.c			2020-05-08 04:05:37 CEST	2020-05-08 04:05:37 CEST	2020-05-08 04:05:37 CEST	2020-05-08 04:0
Microsoft Office 2019.rar.lnk			2020-05-08 03:46:51 CEST	2020-05-08 03:46:51 CEST	2020-05-08 04:52:50 CEST	2020-05-08 03:4
ms-gamingoverlay--kglcheck-.lnk			2020-05-08 03:48:43 CEST	2020-05-08 03:48:43 CEST	2020-05-08 04:52:50 CEST	2020-05-08 03:4
Normal.lnk			2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 04:3
odopen--unlockVault-accounttype=personal.lnk			2020-05-08 05:09:51 CEST	2020-05-08 05:09:51 CEST	2020-05-08 05:09:51 CEST	2020-05-08 05:0
passphrase.lnk			2020-05-08 04:44:03 CEST	2020-05-08 04:44:03 CEST	2020-05-08 04:44:03 CEST	2020-05-08 04:4
project presentation 2020.lnk			2020-05-08 04:20:35 CEST	2020-05-08 04:20:35 CEST	2020-05-08 04:20:35 CEST	2020-05-08 04:0
project2020.lnk			2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 05:37:42 CEST	2020-05-08 04:0
R +D project nov 2020.lnk			2020-05-08 04:20:50 CEST	2020-05-08 04:20:50 CEST	2020-05-08 04:20:50 CEST	2020-05-08 04:0
Templates.lnk			2020-05-08 05:37:43 CEST	2020-05-08 05:37:43 CEST	2020-05-08 05:37:43 CEST	2020-05-08 04:3
The Internet.lnk			2020-05-08 05:09:52 CEST	2020-05-08 05:09:52 CEST	2020-05-08 05:09:52 CEST	2020-05-08 03:4

Figure 23. Shortcut (LNK) Files Artifact in Autopsy



Name	Date modified	Type	Size
AutomaticDestinations	5/14/2020 12:48 PM	File folder	
CustomDestinations	5/14/2020 12:48 PM	File folder	
additional info	5/14/2020 12:48 PM	Shortcut	1 KB
additional info.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
Central_Superstore	5/14/2020 12:48 PM	Shortcut	1 KB
Central_Superstore.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
confidential-projectnovember2020	5/14/2020 12:48 PM	Shortcut	1 KB
confidential-projectnovember2020.lnk-sl...	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
Data	5/14/2020 12:48 PM	Shortcut	1 KB
desktop	5/14/2020 12:48 PM	Configuration sett...	1 KB
Downloads	5/14/2020 12:48 PM	Shortcut	1 KB
Graduation_process	5/14/2020 12:48 PM	Shortcut	1 KB
Graduation_process.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
https--onedrive.live.com-syncru=http%3...	5/14/2020 12:48 PM	Shortcut	2 KB
https--onedrive.live.com-syncru=http%3...	5/14/2020 12:48 PM	LNK-SLACK File	3 KB
Microsoft Office 2019.rar	5/14/2020 12:48 PM	Shortcut	1 KB
Microsoft Office 2019.rar.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
ms-gamingoverlay--kglcheck-	5/14/2020 12:48 PM	Shortcut	1 KB
Normal	5/14/2020 12:48 PM	Shortcut	2 KB
Normal.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	3 KB
odopen--unlockVault-accounttype=pers...	5/14/2020 12:48 PM	Shortcut	1 KB
passphrase	5/14/2020 12:48 PM	Shortcut	1 KB
passphrase.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
project presentation 2020	5/14/2020 12:48 PM	Shortcut	1 KB
project presentation 2020.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
project2020	5/14/2020 12:48 PM	Shortcut	1 KB
project2020.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
R+D project nov 2020	5/14/2020 12:48 PM	Shortcut	1 KB
R+D project nov 2020.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
Templates	5/14/2020 12:48 PM	Shortcut	1 KB
Templates.lnk-slack	5/14/2020 12:48 PM	LNK-SLACK File	4 KB
The Internet	5/14/2020 12:48 PM	Shortcut	1 KB

Figure 24. LNK Files extracted from Autopsy in the investigator's system

5.4.5 E-Mail Messages

Unfortunately, Autopsy was not able to obtain the messages sent by the attacker, but since the account belongs to the company, the CEO authorized the investigator to access the account with its credentials. The messages were sent to another Gmail account, under the name of the randomuserthesis@gmail.com. In these e-mails, the leaked content was found as well.

Figure 25 illustrates the e-mail sent by the attacker with the encrypted data.

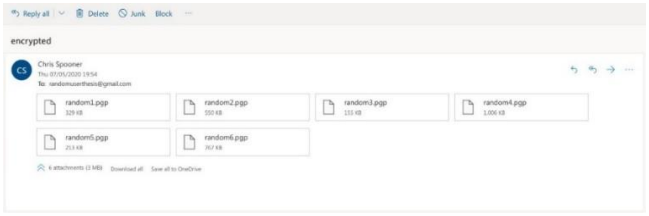


Figure 25. Sent E-Mail Message by the suspect: Encrypted Data

Figure 26 illustrates the e-mail sent by the attacker with the public and private keys for encryption.

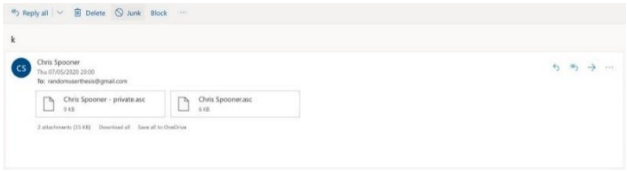


Figure 26. Sent E-Mail Message by the suspect: Public and Private Keys

Figure 27 illustrates the e-mail sent by the attacker with the passphrase for the creation of the keys sent in previous figure.

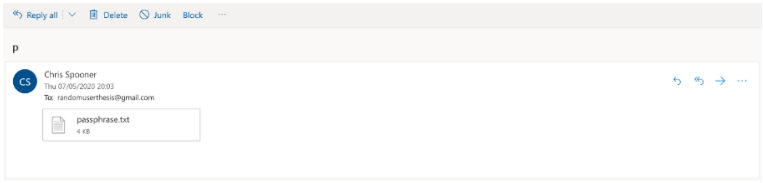


Figure 27. Sent E-Mail Message by the suspect: Passphrase

5.4.6 Tags

When searching for files downloaded by the suspect, the last basic step is where tagging occurs. This is useful to keep track of the different pieces of evidence throughout the investigation and include them in the report that is generated by the software itself.

Figure 28 illustrates the tags added in the case in the software Autopsy.

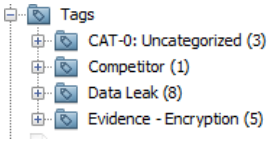


Figure 28. Tags in Autopsy

After digging into all the possible sources of evidence in the system, it was possible to export pictures and videos to the system where Autopsy is locally running.

It was possible to export the encrypted data the attacker sent on the message previously included. Along with the information, the private key, the public key and the passphrase were obtained. By using the PGP Tool, the investigator is able to obtain the decrypted files going through the following steps:

1. Import the suspect's keys into the PGP Tool.
2. Select the file to decrypt.
3. Specify the passphrase included in the file `passphrase.txt`.
4. Select the decrypted file destination.
5. Repeat step 2 according to the number of files to decrypt. Step 4 required if a new destination is desired only.
6. File decrypted.

After decrypting the files, they are collated with the material that is located in the OneDrive shared folder. The original files were provided by Bioerts. There is a change in one file by adding some clarifying notes, which resulted in the file `additionalinfo.pdf`

After the analysis of the data is completed, a report can be generated automatically. Different output formats can be selected as shown in the following figure. This report is going to be included later in the thesis.

Figure 29 illustrates the wizard in software Autopsy to generate a report automatically.

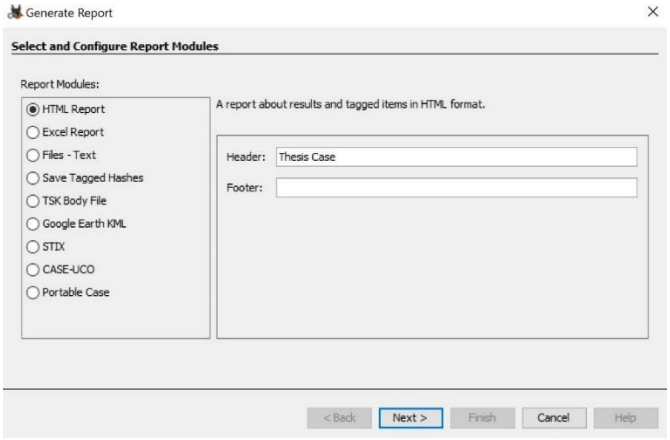


Figure 29. Report Generating Wizard in Autopsy

5.5 Reporting

Report generated by Autopsy included in the "Appendices" chapter.

6 DISCUSSION

With the evolution of communications, starting from the switching systems to the high-tech services present in society nowadays, attempts to break the privacy and security to access unauthorized or confidential content have always accompanied. The evolution of technology has had to go hand in hand with the evolution of laws protecting communications. Thus, emerging new categories of crime in the legal framework. Those in charge of helping in the resolution of this new criminal category, which is cybercrime, are, as previously mentioned, the forensic computer experts.

As stated before in the introduction of this thesis, the world is digitally connected and the flow of information in technological media defines a challenge for regular users of the Internet. Accordingly, the forensic experts must go a step further and expand their skills to analyze and understand its complexity.

It is important to rule out that the fact of introducing more advanced technologies will make it more difficult to guarantee the veracity of the digital evidence in the commission of a crime. In part, this is due to the lack of perception and ignorance that users have of ICT and the interconnected systems that make it possible to interrelate.

For a computer expert, it would be crucial at all times to determine the existence of a crime and who has been responsible. This task becomes more arduous due to the convergence between the real and the virtual world, added to the absence of geographic borders. This gives users *carte blanche* to access content anywhere on the globe.

The problem aggravates the moment in which it damages progress that could benefit scientific research, as is the case in this case study. There is an urgent need to be able to solve such cases. Digital Forensics plays an essential role in bringing attackers to the court and presenting solid, valid, and admissible digital evidence that enables these crimes to be prosecuted. To obtain a conviction, this evidence must have some characteristics. These have been described in this thesis and are a requirement.

In this thesis, an analysis process has been described that follows the standards and complies with the model described in Chapter 3. Having this, admissibility of the evidence that is qualified as accurate and reliable is guaranteed. It is noted that despite the suspect's attempt to erase the evidence after formatting the disk, it has been possible to obtain evidence traces.

After an exhaustive study of the analytical procedure, the requirements of the digital evidence, and the management of the tools to carry out the investigation it has been possible to demonstrate that the crime has taken place, so it is possible to state that the objectives of this thesis have been achieved.

7 CONCLUSION

The thesis has dealt with the supposed obstacles of the constantly changing technology to provide an updated, suitable and admissible analytical framework for a digital forensic analysis carried out by an investigator. It is necessary to consider the possibility of corruption of a case due to mismanagement of the investigation phases. The examination of the digital evidence in the case study was decisive to determine that the offense took place.

The cybercrime chosen for the case study was a “Data Leak/Data Breach” case. The reason behind this choice resides in the importance of this kind of attack entails for almost any company or individual all over the world. It is no news that sensitive data has a price nowadays, and no data category is at no risk of being stolen. This thesis has been able to demonstrate the effectiveness of forensic analysis tools to prove the existence of a computer crime carried out by an attacker. During the course of the investigation, standard documents were also taken into account to assure the digital evidence has the characteristics listed in Chapter 2.

The importance of the results obtained after a digital forensic analysis leads to a decisive point when it comes to proving the innocence or guilt of the suspect. As remarked before, an analysis that does not follow established rules and regulations could stop the prosecution of a truly guilty defendant.

The limitations that may arise may be related to the impossibility of obtaining comprehensive evidence, either due to software limitations or the corruption of the evidence. The greatest advantage is that, along with the advance of information technologies, there is also a leap forward in tools that allow digital forensics experts to carry out more efficient investigations.

The results can be contrasted and analogous to real cases where this type of crime has taken place. Also, the place where this crime has been committed is relevant when undertaking an investigation. One way to continue and extend this work would be taking into account the jurisdiction of the crimes committed since this thesis does not delve deeply into this aspect.

REFERENCES

Panda Security, 2018. *Types of Cybercrime.* [Online]
Available at: https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/
[Accessed 23 03 2020].

Wall, D. S., 2009. What are cybercrimes?. In: *Crime and Deviance in Cyberspace.* 1st ed. s.l.:Ashgate Publishing, p. 16.

Sant, P. & Hewling, M. O., 2011. Digital Forensics: the Need for Integration. In: *Proceedings of the Sixth International Workshop on Digital Forensics & Incident Analysis (WDFIA 2011).* s.l.:University of Plymouth, p. 1.

Vacca, J. & Rudolph, K., 2010. *System Forensics, Investigation and Response (Information Systems Security & Assurance).* 1st ed. s.l.:Jones & Bartlett Learning.

Mayer, R., Rauber, A. & Antunes, G., 2014. *A context model for digital preservation of processes and its application to a digital library system.* s.l., s.n., pp. 459-460.

Sammons, J., 2012. *The basics of digital forensics: the primer for getting started in digital forensics.* 1st ed. s.l.:Elsevier Science & Technology Books.

Chisum, W. J., 1999. *Academy of Behavioral Profiling Annual Meeting.* Monterrey, CA, s.n.

Casey, E., 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* 3rd ed. s.l.:Academic Press.

Hoey, A., 1996. *Analysis of the Police and Criminal Evidence Act, S.69 - Computer Generated Evidence.* s.l.:s.n.

Ahmad, A. & Ruighaver, A., 2004. *Australian Computer, Network & Information Forensics Conference 2004.* Perth, Western Australia, s.n., p. 5.

Sommer, P., 1997. Downloads, Logs and Captures: Evidence from Cyberspace. *Journal of Financial Crime,* Volume 5, pp. 138-151.

Rios, D. J., 2014. *Security Officer Study Guide.* 1st ed. s.l.:Lulu.com.

Benner, J., 2009. Establish a transparent chain-of-custody to mitigate risk and ensure quality of specialized samples. *Biopreservation and biobanking,* 7(3), pp. 151-153.

Jaffee, W. et al., 2008. Focus on alcohol & drug abuse: ensuring validity in urine drug testing. *Psychiatric Services,* 59(2), pp. 140-142.

Tomlinson, J., Elliot-Smith, W. & Radosta, T., 2006. Laboratory information management system chain of custody: Reliability and security. *Journal of Analytical Methods in Chemistry.*

McKemmish, R., 1999. *{What is forensic computing? Trends and issues in crime and criminal justice.* s.l.:Australian Institute of Criminology Canberra.

U.S. Department of Justice Office of Justice Programs, 2004. *National Institute of Justice Annual Report 04.* Washington(DC): National Institute of Justice.

Neijts, R., Semilof, M. & Clark, C., 2018. *TechTarget SearchSecurity.* [Online]
Available at: https://searchsecurity.techtarget.com/definition/steganography
[Accessed 04 04 2020].

Brezinski, D. & Killalea, T., 2002. *RFC 3227. Guidelines for Evidence Collection and Archiving.* [Online]
Available at: https://tools.ietf.org/html/rfc3227
[Accessed 06 04 2020].

ISO/IEC, 2012. *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.* s.l. Patent No. 27037.

Veber, J. & Smunty, Z., 2015. *European Conference on Information Warfare and Security.* s.l., s.n., pp. 294-295.

ISO/IEC, 2015. *Guidance on assuring suitability and adequacy of incident investigative method.* s.l. Patent No. 27041.

ISO/IEC, 2015. *Guidelines for the analysis and interpretation of digital evidence.* s.l. Patent No. 27042.

ISO/IEC, 2015. *Incident investigation principles and processes.* s.l. Patent No. 27043.

ISO/IEC, 2020. *Code of practice for electronic discovery.* s.l. Patent No. 27050-3.

ISO/IEC, 2019. *Overview and concepts.* s.l. Patent No. 27050-1.

The National Institute of Standards and Technology, 2019. *Computer Forensics Tools and Techniques Catalog.* [Online]
Available at: https://toolcatalog.nist.gov/search/index.php
[Accessed 14 04 2020].

WikiPedia, 2020. *Autopsy (software).* [Online]
Available at: https://en.wikipedia.org/wiki/Autopsy_(software)
[Accessed 19 04 2020].

CGSecurity, 2019. *PhotoRec.* [Online]
Available at: https://www.cgsecurity.org/wiki/PhotoRec
[Accessed 23 04 2020].

Access Data Group, Inc., 2016. *Imager User Guide.* s.l.:s.n.

The Volatility Foundation, 2018. *Releases.* [Online]
Available at: https://www.volatilityfoundation.org/
[Accessed 21 04 2020].

Jhala, A. P., n.d. *Digital Evidence - Technical Issues.* [Online]
Available at: http://www.aitd.net.in/pdf/13/12.%20Digital%20%20Evidence-%20Technical%20Issues.pdf
[Accessed 25 03 2020].

Ondata, n.d. *Equipos de Análisis Informático Forense.* [Online]
Available at: https://www.ondata.es/recuperar/computer-forensics.htm
[Accessed 29 04 2020].

ADALID, n.d. *Soluciones en Informática Forense.* [Online]
Available at: https://www.adalid.com/productos/soluciones-en-informatica-forense/
[Accessed 29 04 2020].

Logicube, 2020. *Talon Ultimate.* [Online]
Available at: https://www.logicube.com/shop/talon-ultimate/
[Accessed 29 04 2020].

OpenText, 2020. *Tableau Forensic Imager TX1.* [Online]
Available at: https://www.guidancesoftware.com/tableau/hardware/tx1
[Accessed 29 04 2020].

CRU, 2020. *Ditto.* [Online]
Available at: https://www.cru-inc.com/ditto/
[Accessed 29 04 2020].

Digital Formats, 2019. *Sustainability of Digital Formats: Planning for Library of Congress Collections.* [Online]
Available at: https://www.loc.gov/preservation/digital/formats/fdd/fdd000383.shtml
[Accessed 19 04 2020].

Magnet Forensics, 2014. *Forensic Analysis of LNK files.* [Online]
Available at: https://www.magnetforensics.com/blog/forensic-analysis-of-lnk-files/
[Accessed 19 04 2020].

National Institute of Standards and Technology U.S. Department of Commerce, 2019. *National Software Reference Library (NSRL).* [Online]
Available at: https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl
[Accessed 19 04 2020].

The Sleuth Kit, n.d. *Autopsy.* [Online]
Available at: https://www.sleuthkit.org/autopsy/
[Accessed 19 04 2020].

Prasad, A. & Pandey, J., 2016. *Digital Forensics.* s.l.:Uttarakhand Open University.

Conexión Directa, 2013. *Forensic Powertools Listado de herramientas forenses (List of forensic tools).* [Online]
Available at: http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html
[Accessed 15 04 2020].

Ford, C., 2014. What the Best Evidence Rule is - and what it isn't. *The Scholarly Forum @ Montana Law,* 40(2), p. 22.

The Sleuth Kit, 2016. *Autopsy User Documentation - UI Layout.* [Online]
Available at: https://sleuthkit.org/autopsy/docs/user-docs/4.0/uilayout_page.html
[Accessed 19 04 2020].

Katsavounidis, C., 2018. *Github - kacos2000/WindowsTimeline.* [Online]
Available at: https://kacos2000.github.io/WindowsTimeline/WindowsTimeline.pdf
[Accessed 13 05 2020].

Badiye, A., Kapoor, N. & Menezes, R. G., 2019. *Chain of Custody (Chain of Evidence).* [Online]
Available at: https://www.ncbi.nlm.nih.gov/books/NBK551677/
[Accessed 31 03 2020].

ISO/IEC, 2018. *Guidance for governance and management of electronic discovery.* s.l. Patent No. 27050-2.

APPENDICES

NIST: Computer Forensics Tools and Techniques Catalog

Table 6. Cloud Services Forensic Tools and Techniques

Cloud Services	
Belkasoft Evidence Center	**Version:** 9.7 **Release Date:** October 2019 **Developer:** Belkasoft **Developer Website:** https://belkasoft.com/ **URL to Tool / Technique Description:** https://belkasoft.com/ec **Tool host OS / runtime environment:** Windows **Supported cloud services:** Dropbox, Flickr, Google Drive/Google Docs, Yandex Disk
Magnet AXIOM	**Version:** v1.2.6 **Release Date:** April 2018 **Developer:** Magnet Forensics **Developer Website:** https://www.magnetforensics.com/ **URL to Tool / Technique Description:** https://www.magnetforensics.com/magnet-axiom/ **Tool host OS / runtime environment:** Windows, Mac OS, Linux **Supported cloud services:** Carbonite, Dropbox, Flickr, Google Drive/Google Docs, OneDrive

Table 7. Hardware Write Block Tools and Techniqu

Hardware Write Block	
Forensic ComboDock v5	**Release Date:** September 2012 **Developer:** CRU-DataPort / WiebeTech **Developer Website:** http://www.cru-dataport.com **URL to Tool / Technique Description:** http://www.wiebetech.com/products/Forensic_ComboDock_v5.php **Host access interface:** eSATA, IEEE 1394a (FireWire 400), IEEE 1394b (FireWire 800), USB 2, USB 3 (at native speeds) **Write-blocked interfaces:** IDE/PATA, SATA **Form factor:** standalone device **Hidden sector identification:** hidden sector identification supported **Support for hidden sector access:** support for hidden sector access (HPA & DCO)

Table 8. Forensic File Copy Tools and Technique

Forensic File Copy	
upcopy	**Version:** 18.04 **Release Date:** April 2018 **Developer:** Dan Mares **Developer Website:** http://www.dmares.com **URL to Tool / Technique Description:** http://www.dmares.com/maresware/html/upcopy.htm **Operating System:** Windows **Supported file systems:** FAT12, FAT16, FAT32, NTFS, exFAT **Hash copy verification:** support for verifying copy by hash **Supported hash algorithms:** MD5, SHA1

Table 9. Data Analytics Forensic Tools and Techniques

Data Analytics	
Intella	**Version:** 2.2.1 **Release Date:** January 2008 **Developer:** Vound Software **Developer Website:** https://www.vound-software.com// **URL to Tool / Technique Description:** https://www.vound-software.com/individual-solutions# compare **Tool host OS / runtime environment:** Windows **Supported analytics:** Criminal intelligence
LANGuardian	**Version:** 14.4.2 **Release Date:** August 2018 **Developer:** NetFort **Developer Website:** https://www.netfort.com **URL to Tool / Technique Description:** https://www.netfort.com/languardian/ **Tool host OS / runtime environment:** Linux **Supported analytics:** Criminal intelligence

Table 10. Database Forensic Tools and Techniques

Database	
Belkasoft Evidence Center	**Version:** 9.7 **Release Date:** October 2019 **Developer:** Belkasoft **Developer Website:** https://belkasoft.com/ **URL to Tool / Technique Description:** https://belkasoft.com/ec **Tool host OS / runtime environment:** Windows **Supported database types:** SQLite
ElcomSoft Distributed Password Recovery	**Version:** 4.0 **Release Date:** August 2018 **Developer:** ElcomSoft **Developer Website:** https://www.elcomsoft.com **URL to Tool / Technique Description:** https://www.elcomsoft.com/edpr.html **Tool host OS / runtime environment:** Windows **Supported database types:** Oracle
Intella	**Version:** 2.2.1 **Release Date:** January 2008 **Developer:** Vound Software **Developer Website:** https://www.vound-software.com// **URL to Tool / Technique Description:** https://www.vound-software.com/individual-solutions# compare **Tool host OS / runtime environment:** Windows **Supported database types:** SQLite

Table 11. WiFi Forensics Tools and Techniques

WiFi Forensics	
Elcomsoft Wireless Security Auditor	**Version:** 2.0 **Release Date:** January 2018 **Developer:** ElcomSoft **Developer Website:** https://www.elcomsoft.com **URL to Tool / Technique Description:** https://www.elcomsoft.com/ewsa.html **Tool host OS / runtime environment:** Windows

WiFi Pineapple	**Version:** NANO **Release Date:** September 2016 **Developer:** Hak5 **Developer Website:** https://www.hak5.org/ **URL to Tool / Technique Description:** https://www.wifipineapple.com/ **Tool host OS / runtime environment:** Windows, Mac OS, Linux, Android

Table 12. Memory Capture and Analysis Tools and Techniques

Memory Capture and Analysis	
Active Defense	**Version:** 1.2.5 **Release Date:** January 2008 **Developer:** HBGary **Developer Website:** http://www.hbgary.com **Tool support for binary RAM dump:** tool support for binary RAM dump **Tool support for memory analysis:** tool support for memory analysis **Supported extractable memory objects:** process list, process status (active, hidden, or exited), processes as .exe files, EPROCESS list, kernel module list, driver list, DLL lists, TCPT_OBJECTs, open handles, open files by process, open registry handles by process, open network sockets, open network connections, TCP connections, passwords
Belkasoft Evidence Center	**Version:** 9.7 **Release Date:** October 2019 **Developer:** Belkasoft **Developer Website:** https://belkasoft.com/ **URL to Tool / Technique Description:** https://belkasoft.com/ec **Tool support for binary RAM dump:** tool support for binary RAM dump **Tool support for memory analysis:** tool support for memory analysis **Supported extractable memory objects:** process list, process status (active, hidden, or exited), processes as .exe files, open files by process, browser artifacts (e.g., in-private browsing history), cloud service artifacts (e.g., Dropbox, Flickr, Google Drive), social network artifacts, webmail artifacts (e.g., Gmail, Hotmail, Yahoo), P2P remnants, Instant Messenger histories

Table 13. Image Analysis (Video & Graphics Files) Tools and Techniques

Image Analysis (Video & Graphics Files)	
Amped FIVE	**Release Date:** November 2017 **Developer:** Amped Software **Developer Website:** https://ampedsoftware.com **URL to Tool / Technique Description:** https://ampedsoftware.com/five **Tool host OS / runtime environment:** Windows **Metadata analysis:** support for EXIF, IPTC, XMP metadata and GPS and map view **Camera "fingerprinting":** camera "fingerprinting" and photo analysis not supported **Detecting illicit images:** illicit image detection not supported **Detecting altered images:** altered image detection not supported **Photogrammetry:** photogrammetry supported **Video content analysis:** support for video content analysis **Comparative analysis:** support for comparative analysis
Authenticate	**Release Date:** January 2014 **Developer:** Amped Software **Developer Website:** https://ampedsoftware.com **URL to Tool / Technique Description:** https://ampedsoftware.com/authenticate **Tool host OS / runtime environment:** Windows **Metadata analysis:** support for EXIF, IPTC, XMP metadata and GPS and map view **Camera "finger printing":** support for camera "finger printing" and photo analysis **Detecting illicit images:** support for detecting illicit images **Detecting altered images:** support for detecting altered images **Photogrammetry:** no support for photogrammetry **Video content analysis:** video content analysis not supported **Comparative analysis:** comparative analysis not supported

Table 14. Video Format Conversion Tools and Techniques

Video Format Conversion	
DVRConv	**Release Date:** September 2016 **Developer:** Amped Software **Developer Website:** https://ampedsoftware.com **URL to Tool / Technique Description:** https://ampedsoftware.com/dvrconv **Tool host OS / runtime environment:** Windows **Supported evidence file sources:** CCTVs, DVRs, drones, mobile devices (smartphones, tablets), body worn cameras, consumer cameras, dash cams, IP/IoT cameras, video cameras/camcorders

Table 15. Deleted File Recovery Tools and Techniques

Deleted File Recovery	
Autopsy	**Version:** 3.0 **Release Date:** October 2012 **Developer:** The Sleuth Kit **Developer Website:** http://www.sleuthkit.org/autopsy **Tool host OS / runtime environment:** Windows **Supported file systems:** FAT12, FAT16, FAT32, NTFS, EXT2, EXT3 **Overwritten file identification:** identifying overwritten files unsupported
Disk Drill	**Version:** 3.0 **Release Date:** August 2016 **Developer:** CleverFiles **Developer Website:** http://www.cleverfiles.com/ **Tool host OS / runtime environment:** Windows, Mac **Supported file systems:** FAT12, FAT16, FAT32, NTFS, exFAT, ReFS ,EXT2, EXT3, EXT4 **Overwritten file identification:** identifying overwritten files unsupported.
Magnet AXIOM	**Version:** v1.2.6 **Release Date:** April 2018 **Developer:** Magnet Forensics **Developer Website:** https://www.magnetforensics.com/ **Tool host OS / runtime environment:** Windows, Linux, Mac **Supported file systems:** FAT12, FAT16, FAT32, NTFS, exFAT, ReFS ,EXT2, EXT3, EXT4 **Overwritten file identification:** identifying overwritten files unsupported.
The Sleuth Kit	**Version:** 4.0 **Release Date:** October 2012 **Developer:** The Sleuth Kit **Developer Website:** http://www.sleuthkit.org/sleuthkit **Tool host OS / runtime environment:** Windows, Linux, Mac **Supported file systems:** FAT12, FAT16, FAT32, NTFS, EXT2, EXT3 **Overwritten file identification:** identifying overwritten files unsupported

Table 16. Password Recovery Tools and Techniques

Password Recovery	
Advanced Archive Password Recovery	**Version:** 4.54 **Release Date:** September 2018 **Developer:** Elcomsoft Co. Ltd. **Developer Website:** https://www.elcomsoft.com **URL to Tool / Technique Description:** https://www.elcomsoft.com/archpr.html **Tool host OS / runtime environment:** Windows
Advanced EFS Data Recovery	**Version:** 4.50 **Release Date:** March 2014 **Developer:** Elcomsoft Co. Ltd. **Developer Website:** https://www.elcomsoft.com **URL to Tool / Technique Description:** https://www.elcomsoft.com/aefsdr.html **Tool host OS / runtime environment:** Windows
Advanced SQL Password Recovery	**Developer:** Elcomsoft Co. Ltd. **Developer Website:** https://www.elcomsoft.com **URL to Tool / Technique Description:** https://www.elcomsoft.com/asqlpr.html **Tool host OS / runtime environment:** Windows

Table 17. Disk Imaging Tools and Techniques

Disk Imaging	
Solo-4 Forensics	**Release Date:** September 2008 **Developer:** Intelligent Computer Solutions, Inc **Developer Website:** http://www.ics-iq.com **URL to Tool/Technique Description:** http://www.ics-iq.com/ ImageMASSter-Solo-4-Forensic-Hard-Drive-Duplicator-p/f.gr-0035-000e.htm **Tool host OS / runtime environment:** standalone device **Supported evidence interfaces:** IDE/PATA, SATA, SAS, USB 2, IEEE 1394 (FireWire), CompactFlash **Supported target/destination interfaces:** IDE/PATA, SATA, SAS, CompactFlash, Ethernet **Types of data that may be acquired:** whole drives/devices **Supported acquisition methods:** disk-to-file copy (image), disk-to-disk copy (clone) **Supported image file formats:** raw (dd), Expert Witness (.e01), virtual disk format (e.g., .vdi, .vhd, .vmdk) **Support for restoring the contents of an image file to a device:** image file restore supported, support for restoring a subset of an image file **Digest hash algorithms:** CRC-32, MD5, SHA1, SHA2-256, SHA2-512, SHA3-256, SHA3-512 **Data encryption:** integrated support for data encryption
CFID (Covert Forensic Imaging Device) V3	**Version:** 3 **Release Date:** September 2016 **Developer:** SCG Canada **Developer Website:** http://www.scgcanada.com/ **URL to Tool / Technique Description:** http://www.scgcanada.com/ **Tool host OS / runtime environment:** standalone device (battery powered), custom boot environment (e.g., bootable Linux thumb drive/CD/DVD) **Supported evidence interfaces:** USB 2, USB 3 (at native speeds), SD card **Supported target/destination interfaces:** USB 3 (at native speeds) **Types of data that may be acquired:** whole drives/devices **Supported acquisition methods:** disk-to-file copy (image), disk-to-disk copy (clone) **Supported image file formats:** raw (dd), Expert Witness (.e01), EnCase Evidence File Format Version 2 (.ex01) **Support for restoring the contents of an image file to a device:** image file restore supported **Digest hash algorithms:** MD5, SHA1, SHA2-256 **Data encryption:** no integrated support for data encryption

Table 18. Remote Capabilities/Remote Forensics Tools and Techniques

Remote Capabilities / Remote Forensics	
AD Enterprise	**Developer:** AccessData **Developer Website:** http://www.accessdata.com **URL to Tool / Technique Description:** http://www.accessdata.com/products/digital-forensics/ ad-enterprise **Ability to acquire or analyze live remote data (e.g., connect to and search live remote systems, collect running processes, files, RAM, etc.):** tool support for "live" remote forensics **Ability to acquire or analyze remote data post mortem (e.g., search, preview, or acquire remote hard drive, remote media that has been seized but analyst is accessing it over the network, i.e., remote lab capability):** tool support for "post mortem" remote forensics
Belkasoft Evidence Center	**Version:** 9.7 **Release Date:** October 2019 **Developer:** Belkasoft **Developer Website:** https://belkasoft.com/ **URL to Tool / Technique Description:** https://belkasoft.com/ec **Ability to acquire or analyze live remote data (e.g., connect to and search live remote systems, collect running processes, files, RAM, etc.):** tool support for "live" remote forensics **Ability to acquire or analyze remote data post mortem (e.g., search, preview, or acquire remote hard drive, remote media that has been seized but analyst is accessing it over the network, i.e., remote lab capability):** tool support for "post mortem" remote forensics

Table 19. Video Analytics Tools and Techniques

Video Analytics	
SmartMotion	**Version:** 6.9.1 **Release Date:** January 2015 **Developer:** Jeff Hager **Developer Website:** https://smartmotion.me **URL to Tool / Technique Description:** https://smartmotion.me **Tool host OS / runtime environment:** Windows, Mac OS, Linux **Supported analytics:** object (e.g., person, car) classification and detection, motion detection, tripwires, masking (e.g., privacy)
Video Investigation Portable(VIP)	**Version:** V1.0.15.7996 **Release Date:** May 2015 **Developer:** XLY Salvationdata Technology INC **Developer Website:** http://www.salvationdata.com/ **URL to Tool / Technique Description:** http://www.salvationdata.com/ vip-video-investigation-portable.html **Tool host OS / runtime environment:** Windows **Supported analytics:** object (e.g., person, car) classification and detection, loitering detection, dwell time detection, motion detection, tripwires

Table 20. Email Parsing Tools and Techniques

Email Parsing	
Aid4Mail	**Version:** 2.6 **Release Date:** October 2012 **Developer:** Fookes Software Ltd **Developer Website:** http://www.fookes.com/ **URL to Tool / Technique Description:** http://www.aid4mail.com/ **Tool host OS / runtime environment:** Windows **Supported mail types:** Outlook, Outlook Express, The Bat!, Thunderbird, Eudora, Apple Mail, Windows Mail, Windows Live Mail, Netscape Messenger, Pegasus Mail, Forte Agent, PocoMail, Barca, Calypso, Courier Mail, Opera Mail, FoxMail, maildir, Unix mail (Pine, Elm, mbox, etc.), E-mail file (EML), Webmail (e.g., GMail, Hotmail, Yahoo), Webservices for IMAP access
BlackLight	**Version:** 2015R3.1 **Release Date:** October 2015 **Developer:** BlackBag Technologies **Developer Website:** BlackBagTechnologies **URL to Tool / Technique Description:** https://www.blackbagtech.com/software-products/ blacklight-1/blacklight.html **Tool host OS / runtime environment:** Windows, Mac OS **Supported mail types:** Apple Mail

Table 21. Software Write Block Tools and Techniques

Software Write Block	
DF	**Version:** 1.3 **Release Date:** February 2013 **Developer:** ArxSys **Developer Website:** http://www.arxsys.fr **URL to Tool / Technique Description:** http://www.digital-forensic.org **Tool host OS / runtime environment:** Windows, Linux
SoftBlock	**Version:** 1.0.7 **Release Date:** May 2014 **Developer:** BlackBag Technologies **Developer Website:** https://www.blackbagtech.com **URL to Tool / Technique Description:** https://www.blackbagtech.com/software-products/ softblock-1/softblock.html **Tool host OS / runtime environment:** Mac

Table 22. File Carving Tools and Techniques

File Carving	
OSForensics	**Version:** v4.0.1 **Release Date:** December 2016 **Developer:** PassMark Software **Developer Website:** http://www.passmark.com **URL to Tool / Technique Description:** http://osforensics.com/whatsnew.html **Tool host OS / runtime environment:** Windows **Supported file types:** graphics (e.g., jpg, png, bmp, gif), audio (e.g., mp3, wav, au, wma), video (e.g., mp4, avi, mov, flv), documents (e.g., doc, xls, ppt, pdf), archives (e.g., 7z, bz2, zip, tar) **Custom file types:** support for adding/defining custom file types **Carving boundaries:** support for carving on sector boundaries and cluster boundaries **Supported file carving methods:** support for header/footer-based carving - carving files using a distinct header and footer, header/maximum size carving - carving files using a distinct header and maximum file size, carving fragmented files - two or more fragments are reassembled to form the original file **File viewer/file preview:** integrated file viewer/file preview
PhotoRec	**Version:** 7.0 **Release Date:** April 2015 **Developer:** CGSecurity **Developer Website:** https://www.cgsecurity.org/ **URL to Tool / Technique Description:** https://www.cgsecurity.org/wiki/PhotoRec **Tool host OS / runtime environment:** Windows, Linux, Mac **Supported file types:** graphics (e.g., jpg, png, bmp, gif), audio (e.g., mp3, wav, au, wma), video (e.g., mp4, avi, mov, flv), documents (e.g., doc, xls, ppt, pdf), archives (e.g., 7z, bz2, zip, tar) **Custom file types:** support for adding/defining custom file types **Carving boundaries:** support for carving on sector boundaries and cluster boundaries **Supported file carving methods:** support for header/footer-based carving - carving files using a distinct header and footer, support for header/maximum size carving - carving files using a distinct header and maximum file size, support for file structure-based carving - carving files using a certain level of knowledge of the internal structure of file types, support for carving fragmented files - two or more fragments are reassembled to form the original file, support for carving with file type validation - carved files are validated using a file type specific validator **File viewer/file preview:** no integrated file viewer/file preview

Table 23. Social Media Tools and Techniques

Social Media	
Belkasoft Evidence Center	**Version:** 9.7 **Release Date:** October 2019 **Developer:** Belkasoft **Developer Website:** https://belkasoft.com/ **URL to Tool / Technique Description:** https://belkasoft.com/ec **Tool host OS / runtime environment:** Windows **Supported social media platforms:** Facebook, Flickr, Foursquare, Google+, Instagram, LinkedIn, MySpace, Pinterest, Skype, Telegram, Tumblr, Twitter, Vkontakte
UFED Cloud Analyzer	**Version:** 7.1.0 **Release Date:** March 2018 **Developer:** Cellebrite Ltd. **Developer Website:** https://www.cellebrite.com/ **URL to Tool / Technique Description:** https://www.cellebrite.com/en/products/ ufed-cloud-analyzer/ **Tool host OS / runtime environment:** Windows **Supported social media platforms:** Facebook, Twitter, LinkedIn, Google+, Skype, Telegram, Vkontakte, Instagram, OKCupid

Table 24. Hash Analysis Tools and Techniques

Hash Analysis	
The Sleuth Kit	**Version:** 4.0 **Release Date:** October 2012 **Developer:** The Sleuth Kit **Developer Website:** http://www.sleuthkit.org/sleuthkit **Tool host OS / runtime environment:** Windows, Mac, Linux **Hash computation:** hash files, hash archive file contents **Supported hash algorithms:** MD5, SHA1 **Create and manage hashsets:** support for creating and managing hashsets **Hash search- use of hashes or hash sets to identify files/objects of interest:** search by hash supported **Hash elimination- use of hash sets to filter out files/objects (e.g., "known good" or "known benign" files):** tool support for hash elimination **Hash de-duplication- use of hashes to eliminate identical files/objects:** tool support for hash de-duplication
BlackLight	**Version:** 2015R3.1 **Release Date:** October 2015 **Developer:** BlackBag Technologies **Developer Website:** https://www.blackbagtech.com **URL to Tool / Technique Description:** https://www.blackbagtech.com/software-products/ blacklight-1/blacklight.html **Tool host OS / runtime environment:** Windows, Mac **Hash computation:** hash files, hash e-mails, hash media (e.g., hard drive, thumb drive, partition) **Supported hash algorithms:** MD5, SHA1, SHA2-256, fuzzy hashing – PhotoDNA **Create and manage hashsets:** support for creating and managing hashsets **Hash search- use of hashes or hash sets to identify files/objects of interest:** search by hash supported **Hash elimination- use of hash sets to filter out files/objects (e.g., "known good" or "known benign" files):** tool support for hash elimination **Hash de-duplication- use of hashes to eliminate identical files/objects:** tool support for hash de-duplication
md5.exe	**Version:** 18.03 **Release Date:** March 2018 **Developer:** Dan Mares **Developer Website:** http://dmares.com **URL to Tool / Technique Description:** http://www.dmares.com/maresware/html/md5.htm **Tool host OS / runtime environment:** Windows **Hash computation:** hash files **Supported hash algorithms:** MD5, SHA1, SHA2-256, SHA2-512, SHA3-256, SHA3-512 **Create and manage hashsets:** support for creating and managing hashsets **Hash search- use of hashes or hash sets to identify files/objects of interest:** search by hash supported **Hash elimination- use of hash sets to filter out files/objects (e.g., "known good" or "known benign" files):** tool support for hash elimination **Hash de-duplication- use of hashes to eliminate identical files/objects:** tool support for hash de-duplication

Table 25. Web Browser Forensics Tools and Techniques

Web Browser Forensics	
BURP	**Version:** 1.7.17 **Release Date:** November 2016 **Developer:** PortSwigger Ltd **Developer Website:** https://portswigger.net **URL to Tool / Technique Description:** https://portswigger.net/burp/ **Tool host OS / runtime environment:** Windows, Mac OS, Linux **Supported browsers:** Safari, Bing Toolbar, Firefox, Chrome, Google Maps, Google Toolbar, Internet Explorer, Opera, 360 Safe Browser, Xbox Internet Explorer
Internet Evidence Finder (IEF)	**Version:** v6.8 **Release Date:** September 2016 **Developer:** Magnet Forensics **Developer Website:** http://www.magnetforensics.com **URL to Tool / Technique Description:** http://www.magnetforensics.com **Tool host OS / runtime environment:** Windows, Mac OS, Linux **Supported browsers:** Safari, Bing Toolbar, Firefox, Chrome, Google Maps, Google Toolbar, Internet Explorer, Opera, 360 Safe Browser, Xbox Internet Explorer

Table 26. Mobile Device Acquisition, Analysis and Triage Tools and Techniques

Mobile Device Acquisition, Analysis and Triage	
MPE+ (Mobile Phone Examiner)	**Version:** 5.5 **Release Date:** January 2014 **Developer:** AccessData **Developer Website:** http://www.accessdata.com **URL to Tool / Technique Description:** http://www.accessdata.com/products/digital-forensics/ mobile-phone-examiner **Tool host OS / runtime environment:** Windows **Mobile device data analysis:** tool support for data analysis **3rd party image analysis:** tool support for importing/analyzing 3rd party images **Mobile device acquistion:** mobile device acquistions supported **Supported acquisition types:** logical, physical, manual (i.e., screen capture tool), SIM card **Supported network(s):** GSM network support, non-GSM (i.e., CMDA, iDen) network support **Supported device types:** Smart phone (android) support, Smart phone (iphone) support, Smart phone (Windows Mobile) support, Smart phone (BlackBerry) support, Smart phone (Symbian) support, Smart phone (Palm) support, Tablet (android) support, Tablet (apple) support, Tablet (other) support, non-Smart phone support, Chinese chipset phone (e.g., Mediatek, Spreadtrum, Infineon) support , PDA device support, GPS device support **SIM card cloning:** SIM card cloning supported
Oxygen Forensic Detective	**Version:** 10.2 **Release Date:** April 2018 **Developer:** Oxygen Forensics Inc. **Developer Website:** https://www.oxygen-forensic.com **URL to Tool / Technique Description:** https://www.oxygen-forensic.com/en/products/ oxygen-forensic-detective **Tool host OS / runtime environment:** Windows **Mobile device data analysis:** tool support for data analysis **3rd party image analysis:** tool support for importing/analyzing 3rd party images **Mobile device triage:** tool support for triage **Mobile device acquistion:** mobile device acquistions supported **Supported acquisition types:** logical, physical, manual (i.e., screen capture tool), SIM card **Supported network(s):** GSM network support, non-GSM (i.e., CMDA, iDen) network support **Supported device types:** Smart phone (android) support, Smart phone (iphone) support, Smart phone (Windows Mobile) support, Smart phone (BlackBerry) support, Smart phone (Symbian) support, Smart phone (Palm) support, Tablet (android) support, Tablet (apple) support, Tablet (other) support, non-Smart phone support, Chinese chipset phone (e.g., Mediatek, Spreadtrum, Infineon) support , PDA device support, GPS device support **SIM card cloning:** SIM card cloning unsupported

Table 27. Incident Response Forensic Tracking & Reporting Tools and Techniques

Incident Response Forensic Tracking & Reporting	
Belkasoft Evidence Center	**Version:** 9.7 **Release Date:** October 2019 **Developer:** Belkasoft **Developer Website:** https://belkasoft.com/ **URL to Tool / Technique Description:** https://belkasoft.com/ec **Tool host OS / runtime environment:** Windows

Table 28. Windows Registry Analysis Tools and Techniques

Windows Registry Analysis	
Belkasoft Evidence Center	**Version:** 9.7 **Release Date:** October 2019 **Developer:** Belkasoft **Developer Website:** https://belkasoft.com/ **URL to Tool / Technique Description:** https://belkasoft.com/ec **Tool host OS / runtime environment:** Windows **Input data type(s):** raw (dd), EnCase Evidence File Format Version 2 (.ex01), Expert Witness (.e01), virtual disk format (e.g., .vdi, .vhd, .vmdk), physically mounted slave drive **Automated hive extraction and parsing:** active Registry, active file system, volume shadow copies, unallocated space **Registry rebuilding:** Registry rebuilding unsupported **Deleted key recovery:** supports deleted key recovery **Key and value instance display:** supports display of key and value instances **Pre-built reports:** pre-built reports not supported
Registry Recon	**Version:** 2.10.0015 **Release Date:** November 2014 **Developer:** Arsenal Recon **Developer Website:** http://ArsenalRecon.com **URL to Tool / Technique Description:** http://ArsenalRecon.com/apps **Tool host OS / runtime environment:** Windows **Input data type(s):** raw (dd), EnCase Evidence File Format Version 2 (.ex01), Expert Witness (.e01), virtual disk format (e.g., .vdi, .vhd, .vmdk), physically mounted slave drive, loose hive(s) **Automated hive extraction and parsing:** active Registry, active file system, Windows restore points, volume shadow copies, unallocated space **Registry rebuilding:** Registry rebuilding unsupported **Deleted key recovery:** supports deleted key recovery **Key and value instance display:** supports display of key and value instances **Pre-built reports:** support for pre-built reports

Table 29. Steganalysis Tools and Techniques

Steganalysis	
Steganography Analyzer Artifact Scanner (StegAlyzerAS)	**Version:** 3.9 **Release Date:** March 2013 **Developer:** Backbone Security - Steganography Analysis and Research Center (SARC) **Developer Website:** http://www.sarc-wv.com **URL to Tool / Technique Description:** http://www.sarc-wv.com/products/stegalyzeras/learn_more. aspx **Tool host OS / runtime environment:** Windows
Steganography Analyzer Field Scanner (StegAlyzerFS)	**Version:** 1.0 **Release Date:** January 2013 **Developer:** Backbone Security - Steganography Analysis and Research Center (SARC) **Developer Website:** http://www.sarc-wv.com **URL to Tool / Technique Description:** http://www.sarcwv.com/products/stegalyzeras/learn_more. aspx **Tool host OS / runtime environment:** Windows
Steganography Analyzer RealTime Scanner (StegAlyzerRTS)	**Version:** 3.3 **Release Date:** June 2012 **Developer:** Backbone Security - Steganography Analysis and Research Center (SARC) **Developer Website:** http://www.sarc-wv.com **URL to Tool / Technique Description:** http://www.sarc-wv.com/products/stegalyzeras/learn_more. aspx **Tool host OS / runtime environment:** network appliance
Steganography Analyzer Signature Scanner (StegAlyzerSS)	**Version:** 3.9 **Release Date:** March 2013 **Developer:** Backbone Security - Steganography Analysis and Research Center (SARC) **Developer Website:** http://www.sarc-wv.com **URL to Tool / Technique Description:** http://www.sarc-wv.com/products/stegalyzeras/learn_more. aspx **Tool host OS / runtime environment:** Windows

Table 30. String Search Tools and Techniques

String Search	
Autopsy	**Version:** 3.0 **Release Date:** October 2012 **Developer:** The Sleuth Kit **Developer Website:** http://www.sleuthkit.org/autopsy **Tool host OS / runtime environment:** Windows **Available search technologies:** Support for indexed search **Advanced search features:** keyword search, regular expression/pattern search **Integrated support for code pages and extended character set encodings:** integrated tool support for code pages and extended character set encodings **Target search areas:** search support for unallocated space, files, files names, files within archive and container files and email search
Belkasoft Evidence Center	**Version:** 9.7 **Release Date:** October 2019 **Developer:** Belkasoft **Developer Website:** https://belkasoft.com/ **URL to Tool / Technique Description:** https://belkasoft.com/ec **Tool host OS / runtime environment:** Windows **Available search technologies:** Support for indexed search **Advanced search features:** keyword search, regular expression/pattern search, hex search **Integrated support for code pages and extended character set encodings:** integrated tool support for code pages and extended character set encodings **Target search areas:** search support for unallocated space, files, files names, files within archive and container files, file slack, internet history and email search
dtSearch Product Line	**Version:** Current version 7.70 **Release Date:** June 2012 **Developer:** dtSearch Corp. **Developer Website:** http://www.dtsearch.com **URL to Tool / Technique Description:** http://www.dtsearch.com/PLF_forensics_2.html **Tool host OS / runtime environment:** Windows, Linux **Available search technologies:** Support for indexed search and live/simultaneous search **Advanced search features:** keyword search, regular expression/pattern search, stemming search, phonetic search, fuzzy search, synonym search **Integrated support for code pages and extended character set encodings:** integrated tool support for code pages and extended character set encodings **Target search areas:** files, files names, files within archive and container files and email search
BlackLight	**Version:** 2015R3.1 **Release Date:** October 2015 **Developer:** BlackBag Technologies **Developer Website:** https://www.blackbagtech.com **URL to Tool / Technique Description:** hhttps://www.blackbagtech.com/software-products/blacklight-1/blacklight.html **Tool host OS / runtime environment:** Windows, Mac **Available search technologies:** Support for live/simultaneous search **Advanced search features:** keyword search, regular expression/pattern search **Integrated support for code pages and extended character set encodings:** integrated tool support for code pages and extended character set encodings **Target search areas:** search support for unallocated space, files, files names, files within archive and container files, file slack, internet history and email search

Other Forensics Tools

Besides the software listed in the tables mentioned earlier, there are several open-source tools available in the market that could do the work in the analysis process (Conexión Directa, 2013)

Acquisition and Memory Analysis

Set of utilities that allow the acquisition of the RAM to later analyze it.

- **pd** - Converts a process from memory to file.
- **FTK Imager** - It allows, among other things, to acquire memory.
- **RedLine** - It captures the memory and allows it to be analyzed. It has a graphic environment.
- **Memoryze** - It captures the RAM

Disk Mounting

Utilities to mount disk images or virtualize drives so that users have access to the file system to later analyze it.

- **ImDisk** - Converts a process from memory to file.
- **OSFMount** - Allows the user to mount images from local disks in Windows by assigning a drive letter.
- **raw2vmdk** - Java utility that allows the user to convert raw / dd to .vmdk.
- **LiveView** - Java utility that creates a VMware virtual machine from a disk image.
- **MountImagePro** - Mount images from local disks in Windows by assigning a drive letter
- **FTK Imager** - Discussed above, allows mounting of disks.

Carving and Disk Tools

Recovery of lost, deleted data, search for patterns and files with certain content such as images, videos. Partition recovery and treatment of disk structures.

- **NTFS Recovery** - Allows data and disk recovery even after disk formatting.
- **Recuva** - Utility for recovering deleted files
- **RAID Reconstructor** - Recover data from a broken RAID, both in raid 5 or raid 0. Even if we do not know the RAID parameters.
- **CnW Recovery** - Recovers corrupt sectors and incorporates carving utilities.
- **Restoration** - Utility for recovering deleted files.
- **R-STUDIO** - Data recovery from any disk system NTFS, NTFS5, ReFS, FAT12 / 16/32, exFAT, HFS / HFS + (Macintosh), Little and Big Endian in their different UFS1 / UFS2 variations (FreeBSD / OpenBSD / NetBSD / Solaris) and Ext2 / Ext3/ Ext4 FS partitions.
- **FreeRecover** - Utility for recovering deleted files.
- **DMDE** - Supports FAT12 / 16, FAT32, NTFS, and works under Windows 98 / ME/

2K / XP / Vista / 7/8 (GUI and console), DOS (console), Linux (Terminal) and incorporates carving utilities.
- **Internet Evidence Finder** - Carving on a disk image looking for more than 230 applications such as google chat, Facebook, IOS, ram memory, virtual memory, etc.
- **Bulk Extractor** - Allows data extraction from images, folders and files.

File System Utilities

Set of tools for data analysis and essential files in the search for an incident.

- **analyzeMFT** - David Kovar's python utility to extract MFT.
- **WinPrefetchView** - Extract and parse the prefetch directory
- **FileASSASSIN** - Unlock files blocked by programs.

Malware Analysis

- **PDF Tools** - This tool will parse a PDF document to identify the fundamental elements used in the analyzed file.
- **PDF Stream Dumper** - This is a free tool for the analysis of malicious PDF documents. Has specialized tools for dealing with obfuscated javascript, low-level pdf headers and objects, and shellcode.
- **SWF Mastah** - Python program that extracts SWF stream from PDF files.
- **Process Explorer** - It shows process information.
- **Regshot** - It creates snapshots of the registry being able to compare the changes between them.
- **LordPE** - Tool to edit certain parts of executables and memory dump of executed processes.
- **Firebug** - Analysis of web applications.
- **IDA Pro** - Application Debugger.
- **OllyDbg** - Disassembler and debugger for applications or processes.
- **jsunpack-n** - It emulates the functionality of the browser when visiting a URL. Its purpose is the detection of exploits.
- **OfficeMalScanner** - It is a forensic tool whose purpose is to search for malicious programs or files in Office.
- **Radare** - Framework for reverse engineering use.
- **FileInsight** - Framework for reverse engineering use.
- **Volatility** - Framework with malfind2 plugins and apihooks.
- **shellcode2exe** - Converter for shellcodes into binaries.

Frameworks

A standardized set of concepts, practices and criteria based on the forensic analysis of a case.

- **log2timeline-Plaso** - Tool designed to extract timestamps from various files found on a typical computer system(s) and aggregate them.
- **SANS SIFT Workstation** - It can match any current incident response and forensic tool suite.

Windows Registry Analysis

It allows obtaining registry data such as users, permissions, executed files, system information, IP addresses, application information.

- **RegRipper** - It is an application to extract, correlate, and display registry information.
- **Windows Registry Recovery** - It allows graphically obtaining data from the system, users and applications from the registry.

Network Tools

It allows obtaining registry data such as users, permissions, executed files, system information, IP addresses, application information.

- **Wireshark** - Tool for capturing and analyzing network packets.
- **NetworkMiner** - Forensic tool for discovering network information.
- **RSA Netwitness Platform** - Forensic Tool. The 'free edition' version is limited to 1GB of traffic.
- **Network Appliance Forensic Toolkit** - Set of utilities for network acquisition and analysis.
- **Snort** - Intrusion Detector. It allows packet capture and analysis.
- **Splunk** - It is the engine for the data and logs generated by the devices, stations and servers. Index and take advantage of data generated by all IT systems and infrastructure: whether physical, virtual or in the cloud.

Password Recovery

Everything related to the recovery of passwords in Windows, by brute force, in forms, in browsers, etc.

- **Ntpwedit** - It is a password editor for Windows NT based systems (like Windows 2000, XP, Vista, 7 and 8), the user can change or delete passwords for local system accounts. Not valid for Active Directory.
- **Ntpasswd** - It is a password editor for Windows-based systems, it allows starting the utility from a CD-LIVE
- **pwdump7** - Dump the hashes. It is executed by extracting the SAM binaries.
- **L0phtcrack** - Dump the hashes. They include dictionaries for brute force attacks.
- **OphCrack** - Dump the hashes. They include dictionaries for brute force attacks.

Mobile Devices

- iPhone
  - **iPhoneBrowser** - Access to the iPhone file system in a graphical environment.
  - **iPhone Analyzer** - It explores the internal file structure of the iPhone.
  - **iPhone Backup Extractor** - It extracts files from a previously made backup.
  - **iPhone Backup Browser** - Extract files from a previously made backup.
  - **iphone-dataprotection** - It contains tools to create a forensic RAM disk, brute force with simple passwords (4 digits) and decrypt backups.
  - **SpyPhone** - It explores the internal file structure.
- Android
  - **android-locdump** - It allows obtaining geolocation information.
  - **androguard** - Allows obtaining, modification and disassembly of DEX / ODEX/ APK / AXML / ARSC formats.
  - **android-forensics** - Utility framework for forensic analysis.

Autopsy – Installation and User Guide

All the information included is extracted from (The Sleuth Kit, n.d.)

- **Windows**
  1. Run the Autopsy msi file.
  2. If Windows prompts with User Account Control, click Yes
  3. Click through the dialog boxes until the Finish button appears in the wizard.
  4. Autopsy should now be fully installed
- **Mac OS X**
  1. Prerequisites
     - Install testdisk for photorec functionality.
       ```
       % brew install testdisk
       ```
     - Install the BellSoft Java 8 JRE and JavaFX 8 distribution and set JAVA_HOME.
       a) Install BellSoft Java 8
       ```
       % brew tap bell-sw/liberica

       % brew cask install liberica-jdk8-full
       ```
       b) Set JAVA_HOME environment variable to location of JRE installation. e.g. add the following to `~/.bashrc` `export JAVA_HOME=$(/usr/libexec/java_home -v 1.8)`
     - Confirm Java version
  2. Install The Sleuth Kit Java Bindings
     Install The Sleuth Kit from brew
     ```
     % brew install sleuthkit
     ```
  3. Install Autopsy
     - Extract the contents of the Autopsy ZIP file to a folder.
     - Open a terminal and cd into the Autopsy folder.
     - Run the unix_setup.sh script to configure Autopsy
     - `% sh unix_setup.sh`
  4. Running Autopsy
     - In a terminal, change to the 'bin' directory in the Autopsy folder.
     - Run Autopsy
       ```
       % ./autopsy
       ```
- **Linux**
  1. Prerequisites
     - Install testdisk for photorec functionality.
       ```
       % sudo apt-get install testdisk
       ```
     - Install the BellSoft Java 8 JRE and JavaFX 8 distribution and set JAVA_HOME.
       a) Install BellSoft Java 8
       ```
       % wget -q -O - https://download.bell-sw.com/pki/GPG-KEY-bellsoft
       | sudo apt-key add -
       % echo "deb [arch=amd64] https://apt.bell-sw.com/ stable main"
       | sudo tee /etc/apt/sources.list.d/bellsoft.list
       % sudo apt-get update
       % sudo apt-get install bellsoft-java8-full
       ```
       b) Set JAVA_HOME
       ```
       % export JAVA_HOME=/usr/lib/jvm/bellsoft-java8-full-amd64
       ```

- Confirm Java version
  ```
  % java -version
  ```

2. Install The Sleuth Kit Java Bindings
   Install the sleuthkit-java.deb file that can be downloaded from https://www.github.com/sleuthkit/sleuthkit/releases. This will install libewf, etc.
   ```
   % sudo apt install ./sleuthkit-java_4.7.0-1_amd64.deb
   ```
3. Install Autopsy
   - Extract the contents of the Autopsy ZIP file to a folder.
   - Open a terminal and cd into the Autopsy folder.
   - Run the unix_setup.sh script to configure Autopsy
     ```
     % sh unix_setup.sh
     ```
4. Running Autopsy
   - In a terminal, change to the 'bin' directory in the Autopsy folder.
   - Run Autopsy
     ```
     % ./autopsy
     ```

Autopsy Workflow

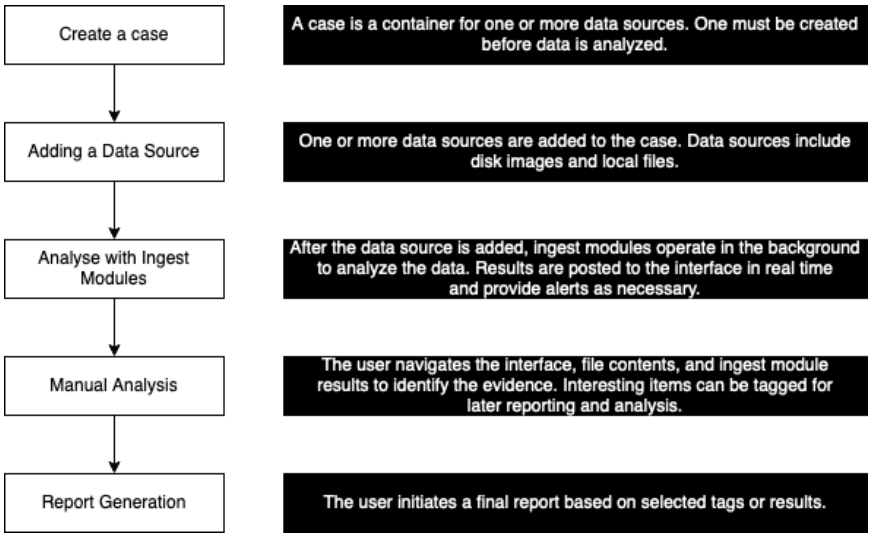


Figure 30. Autopsy Workflow

Analysis Modes

Autopsy includes two analysis modes:

Dead analysis This sort of analysis takes place when a dedicated analysis system is handled to examine the data from a suspect system. The location chosen by the examiner to perform this analysis with both Autopsy and/or The Sleuth Kit must be a trusted laboratory. Autopsy and TSK support raw, Expert Witness, and AFF file formats.

Live analysis This sort of analysis is performed when the suspect system is still running. There exists a big difference between this kind of analysis and the one mentioned above, in this case, Autopsy and The Sleuth Kit are run from a CD in an untrusted environment. This is generally performed during incident response at the same

time the incident is being confirmed. After final confirmation, acquisition materializes, and a dead analysis can be performed.

Input Formats

Autopsy analyzes disk images, local drives, or a folder of local files. Disk images can be in either raw/dd or E01 format (Encase Image File Format).

Analysis Features

Multi-User Cases It is typical that numerous examiners work on the same case simultaneously. Therefore, with Autopsy, it is possible to create multi-user cases to be able to see the results that appear in the investigation found by the different examiners in real-time. To achieve a multi-user environment, it is necessary to use Central PostgreSQL database, Central Apache Solr server, Central Apache ActiveMQ messaging server and Central storage.

Timeline Analysis This feature is useful for a variety of investigation types. Essentially, is used to find out when a computer is used and what events occurred before or after. In order to obtain the full information, several locations are examined such as files, web artifacts and other Autopsy extracted data, such as EXIF and GPS. There are two interfaces available while using this feature. The first one is a bar chart that shows how much data occurred in a given time frame.

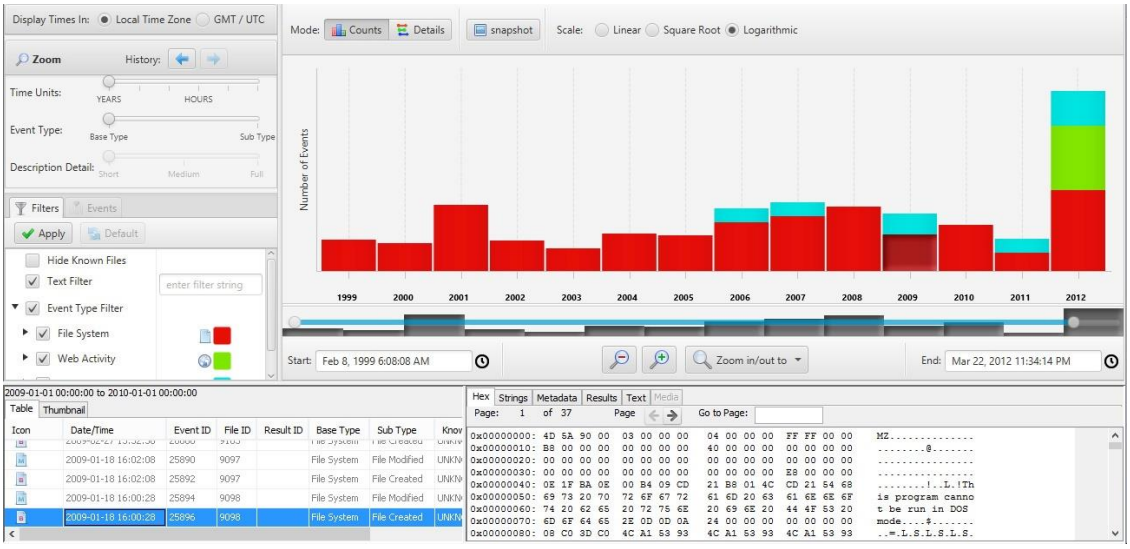


Figure 31. Timeline Analysis' First Interface. Picture downloaded from https://www.sleuthkit. org/autopsy/timeline.php

The second interface gives more details about the events that took place. It has a unique approach of clustering similar events together to prevent data overload.

"For example, all files in the same folder are shown as a single event and all URLs from the same domain are shown as a single event. If the user wants to see more details

about that folder or domain, then they can zoom into it. Otherwise, it is hidden."

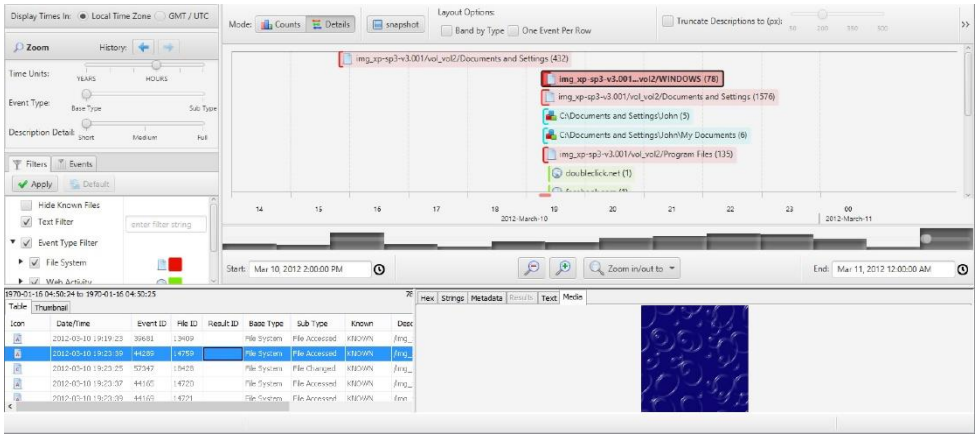


Figure 32. Timeline Analysis' Second Interface. Picture downloaded from https://www.sleuthkit.org/autopsy/timeline.php

Web Artifacts Autopsy is configured to search for common web artifacts from major browsers, such as Firefox, Chrome and Internet Explorer. It extracts information such as bookmarks, cookies, history, downloads and search queries.

With a view to simplifying the data search, all the results from all browsers are merged. If the examiner needs to see a user's history, it is as easy as checking the "History" node. There is no need in going through the different folders for different browsers.

All the results found are categorized and displayed automatically in the Autopsy tree view under the 'Results' node.

Registry Analysis Uses RegRipper to identify recently accessed documents and USB devices.

LNK File [5] Analysis Identifies short cuts and accessed documents

Email Analysis Parses MBOX [6] format messages, such as Thunderbird.

EXIF Extracts geolocation and camera information from JPEG files.

Media Playback Visualize videos and images in the application and not require an external viewer.

---

[5] "They are shortcut files that link to an application or file commonly found on a user's desktop, or throughout a system and end with an .LNK extension. LNK files can be created by the user, or automatically by the Windows operating system. Each has their own value and meaning. Windows-created LNK files are generated when a user opens a local or remote file or document, giving investigators valuable information on a suspect's activity." (Magnet Forensics, 2014)

[6] "MBOX formats store all of the messages of an entire folder (not an entire mailbox) in a single database file and new messages are appended to the end of the file." (Digital Formats, 2019)

Thumbnail viewer Displays thumbnail of images to help quick view pictures.

Robust File System Analysis Support for common file systems, including NTFS, FAT12/ FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS from The Sleuth Kit.

Hash Set Filtering Filter out known good files using NSRL [7] and flag known bad files using custom hash sets in HashKeeper, md5sum, and EnCase formats.

Tags Tag files with arbitrary tag names, such as 'bookmark' or 'suspicious', and add comments.

Unicode Strings Extraction Extracts strings from unallocated space and unknown file types in many languages (Arabic, Chinese, Japanese, etc.).

Interesting Files Module It will flag files and folders based on name and path.

Android Support Extracts data from SMS, call logs, contacts, Tango, Words with Friends, and more.

Evidence Search Techniques

File Listing Analysis of files and directories, including the names of deleted files and files with Unicode-based names.

File Content The contents of files can be viewed in raw, hex, or the ASCII strings can be extracted. After data is interpreted by the software, it is sanitized to avoid any damage to the local analysis system.

Hash Databases Autopsy uses the NIST National Software Reference Library (NSRL) and user-created databases of known good and known bad files to quickly identify its nature.

File Type Sorting It is performed based on their internal signatures. The extension of the file will also be compared to the file type to identify if there was any possible change to try to hide the file.

[7] "The National Software Reference Library (NSRL) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information." (National Institute of Standards and Technology U.S. Department of Commerce, 2019)

Timeline of File Activity Autopsy can create timelines that contain entries for the Modified, Access, and Change (MAC) times of both allocated and unallocated files.

Keyword Search Text indexing engine Apache SOLR is used in order to power Autopsy's fast and robust keyword searching features. Pre-defined lists of keywords and regular expressions can be configured to run while the image is being ingested. By default, Autopsy includes regular expression searches for e-mail addresses, phone numbers, IP addresses and URLs.

Ad hoc keyword searches can be performed directly from the contents bar until (or also during) the disk image is ingested. The database search can be conducted for several parallel keyword searches.

The analysis of the keywords in Autopsy is performed with on the output of text extraction modules instead of on raw data. With the help of Tika and other libraries, Autopsy can extract text from HTML, Microsoft Office, PDF, RTF, and more. This technique is more efficient at finding text than the byte-level searching for non-English PDF files and docx files whereby the data is compressed.

The 'Keyword Hits' node in the Autopsy Navigation tree displays every outcome from the enabled searches (regular expression or user-defined lists). All Autopsy files which contain text contents are indexed to search by the preset regular expression list, user-provided keyword lists or ad hoc queries thanks to Apache SOLR.

Meta Data Analysis Autopsy allows the user to view the details of any metadata structure in the file system. This will come handy for examiners when recovering deleted content. Autopsy will search the directories to identify the full path of the file that has allocated the structure.

Data Unit Analysis File content is stored in Data Units. Autopsy allows viewing the contents of any data unit in a variety of formats including ASCII, hexdump, and strings.

Image Details File system details can be viewed, including on-disk layout and times of activity.

Case Management

Case Management "Investigations are organized by cases, which can contain one or more hosts. Each host is configured to have its own time zone setting and clock skew so that the times shown are the same as the original user would have seen. Each host can contain one or more file system images to analyze."

Event Sequencer "Time-based events can be added from file activity or IDS and firewall logs. Autopsy sorts the events so that the sequence of incident events can be more easily determined."

Notes They can be saved on a per-host and per-investigator basis. These allow the user to make quick notes about files and structures. The original location can be easily recalled with the click of a button when the notes are later reviewed. All notes are

stored in an ASCII file. "

Image Integrity "It is crucial to ensure that files are not modified during analysis. Autopsy, by default, will generate an MD5 value for all files that are imported or created. The integrity of any file that Autopsy uses can be validated at any time."

Reports There is a possibility to create ASCII reports for files and other file system structures. With this feature, it is possible to keep track of consistent datasheets throughout the course of the investigation.

Logging Audit logs are created on a case, host, and investigator level so that actions taken during the analysis are registered and can be recalled. The exact Sleuth Kit commands that are executed are also logged.

Open Design "The code of Autopsy is open source and all files that it uses are in a raw format. All configuration files are in ASCII text and cases are organized by directories. This makes it easy to export the data and archive it. It also does not restrict the user from using other tools that may solve the specific problem more appropriately."

Client Server Model "Autopsy is HTML-based and therefore the user does not have to be on the same system as the file system images. This allows multiple investigators to use the same server and connect from their personal systems."

Reporting

Autopsy has an extensible reporting infrastructure that allows additional types of reports for investigations to be created. By default, HTML, XLS, and Body file reports are available. Each one is configurable depending on what information an investigator would like included in their report:

HTML and Excel The HTML and Excel reports are intended to be fully packaged and shareable reports. They can include references to tagged files along with comments and notes inserted by the investigator as well as other automated searches that Autopsy performs during ingest. These include bookmarks, web history, recent documents, keyword hits, hashset hits, installed programs, devices attached, cookies, downloads, and search queries.

Body File Primarily for use in timeline analysis, this file will include MAC times for every file in an XML format for import by external tools, such as mactime in The Sleuth Kit.

An investigator can generate more than one report at a time and either edit one of the existing or create a new reporting module to customize the behavior for their specific needs.

User Interface (UI) Layout

In the current subsection the major areas in the Autopsy User Interface in a Windows

Operating System. The information displayed, text and figures, are extracted from (The Sleuth Kit, 2016).

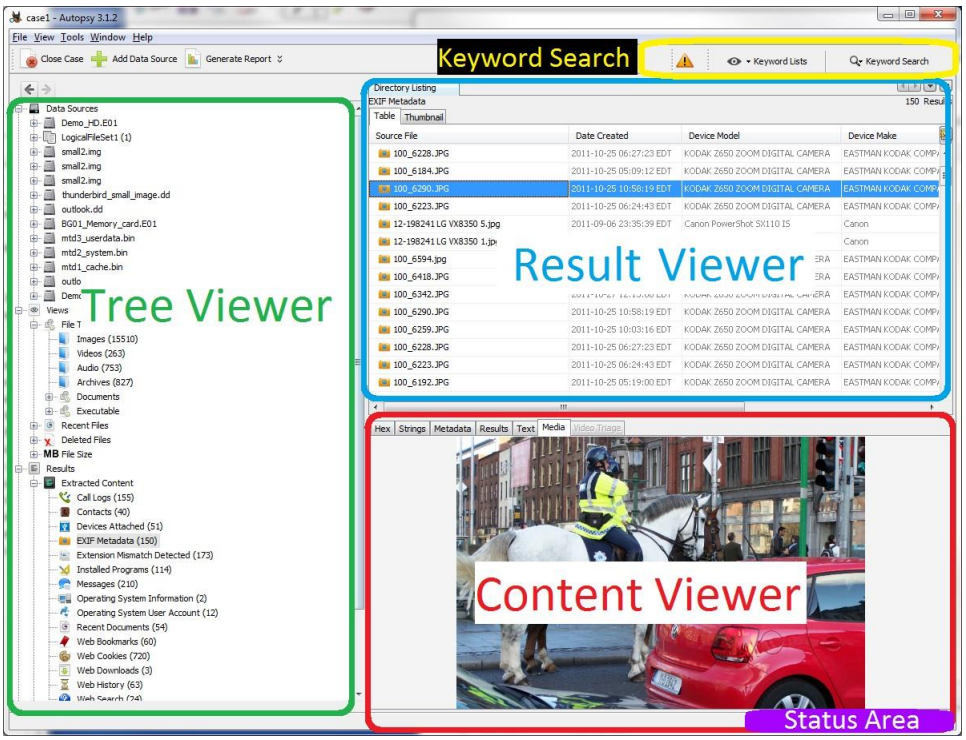


Figure 33. Autopsy's User Interface

- **Tree Viewer:** It is responsible for showing the discovered folders by data sources they come from, as well as a list of files in the folders. The number of items contained in each folder is specified in the number within parenthesis following the name of it.

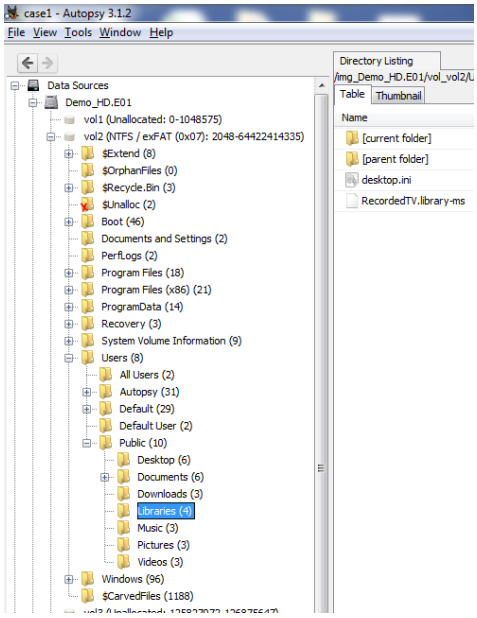


Figure 34. Tree Viewer example

The tree has four main areas which are the following:

Data Sources: As its name implies, this section will show the different data sources that have been added to the case. By right-clicking on the nodes it is possible to have more options for each data source and its contents.

It is important to know what "unallocated space" is in this context, it refers to chunks of the file system that is currently not being used for anything that can store deleted files and other interesting artifacts. This unallocated space can be stored in blocks but also in a single large unallocated file. Autopsy provides access to both methods of looking at unallocated space.

- **Individual block in a volume:** There is a folder named "Unalloc". This folder contains all the individual unallocated blocks as the image is storing them. By right-clicking, it is possible to extract these blocks the same way any other type of file in the Directory Tree.
- **Single files:** In the figure below, it is shown how to extract to a single file after right-clicking on a volume. By selecting "Extract Unallocated Space as Single File" it concatenates all the unallocated files in the volume into a single, continuous file.

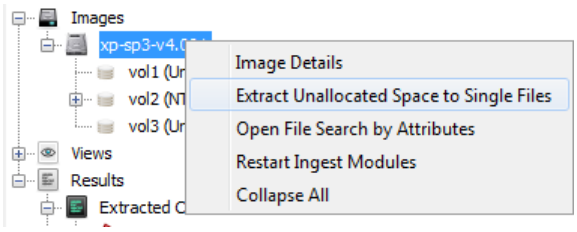


Figure 35. Single File Extraction

Views: It filters all the files in the case by some external property of the file, not by

any internal analysis of the file.

- **File Type Sorts:** files by file extension and shows them in the appropriate group.
- **Recent Files:** Displays files that are accessed within the last seven days the user had the device.
- **Deleted Files:** Displays files that have been deleted but the names have been recovered.
- **File Size Sorts:** files based upon size.

Results

- **Extracted Content:** Many ingest modules will place results here.
- **Keyword Hits:** Keyword search hits show up here
- **Hashset Hits:** Hashset hits show up here
- **E-Mail Messages:** Email messages show up here
- **Interesting Items:** Evidence deemed interesting show up here
- **Tags:** Any item the user tags shows up here so it is found easily again later.

Reports: Reports can be added by Ingest Modules or created using the Reporting tool.

- **Result Viewer:** It shows lists of files and their corresponding attributes such as time, path, size, checksum, etc. There is a variety of formats in which the results can be visualized.

Thumbnail Result Viewers: This format displays the data catalog as a table of thumbnail images in adjustable sizes. This viewer only supports picture files (Currently, only supports JPG, GIF, and PNG formats).

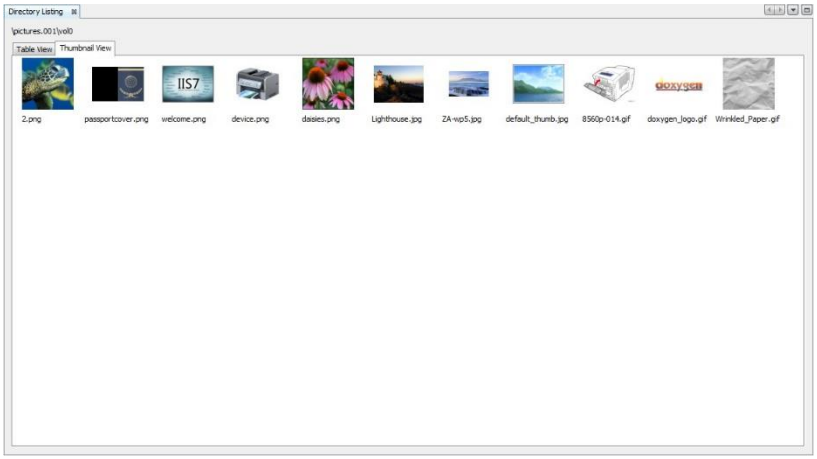


Figure 36. Example of "Thumbnail Results Viewer"

Table Result Viewers: This format displays the data catalog as a table with some details (properties) of each file. The properties that it shows are name, time (modified, changed, accessed, and created), size, flags (directory and meta), mode, user ID, group ID, metadata address, attribute address, and type (directory and meta).

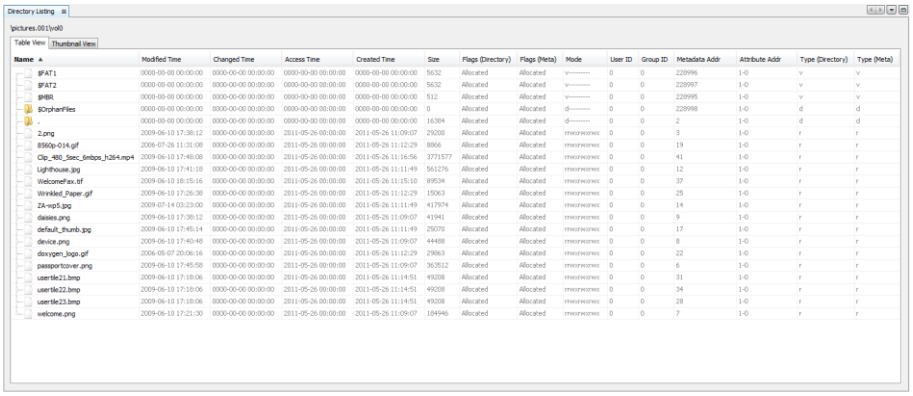


Figure 37. Example of "Table Results Viewer"

Additionally, Viewers in Result Viewers have several right-click functions built-in into them that can be accessed when a node a certain type is selected (a file, directory or a result). These are some examples:

- Open File in External Viewer: Opens the selected file in an "external" application as defined by the local OS.
- View in New Window: Opens the content in a new internal Content Viewer (instead of in the default location in the lower right).
- Extract: Make a local copy of the file or directory for further analysis.
- Search for files with the same MD5 Hash: Searches the entire file system for any files with the same MD5 Hash as the one selected.

- **Content Viewer:** Area used to view a specific file in a variety of formats. There are different tabs for different viewers. To display data in this area, a file must be selected from the Result Viewer window.

  Result Content Viewer: It shows the artifacts (saved results) associated with the item selected in the Result Viewer.

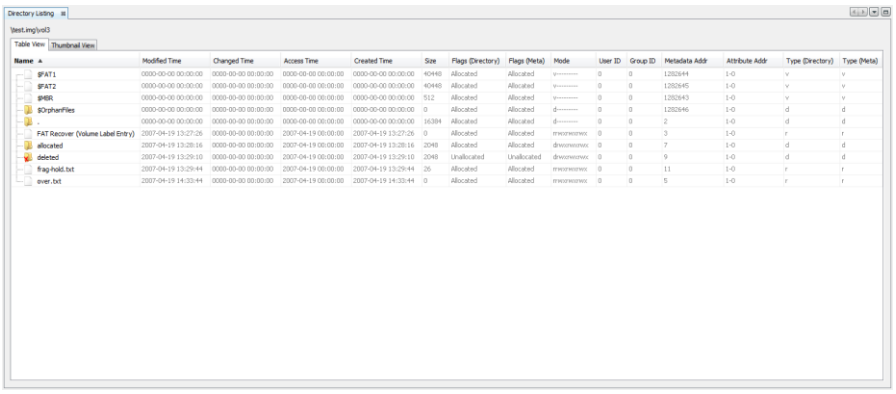


Figure 38. Example of "Result Content Viewer"

Hex Content Viewer: It shows the raw and exact contents of a file. In this Hex

Content Viewer, the data of the file is represented as hexadecimal values grouped in 2 groups of 8 bytes, followed by one group of 16 ASCII characters that are derived from each pair of hex values (each byte). Non- printable ASCII characters and characters that would take more than one character space are typically represented by a dot (".") in the following ASCII field.

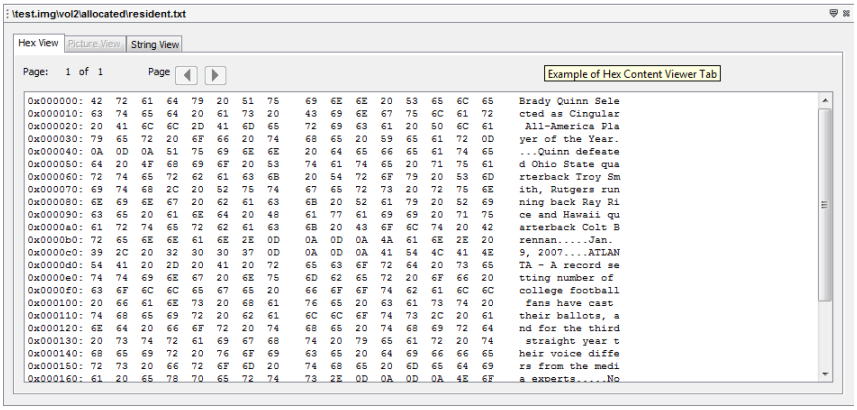


Figure 39. Example of "Hex Content Viewer"

Media Content Viewer: It shows a picture or video file. Video files can be played and paused. The size of the picture or video will be reduced to fit into the screen. If a more complex analysis is required, the examiner must export the file.

Figure 40. Example of "Media Content Viewer"

String Content Viewer: It scans (potentially binary) data of the file/folder and searches it for data that could be text. When appropriate data is found, the String Content Viewer shows data strings extracted from binary, decoded, and interpreted as UTF8/16 for the selected script/language.

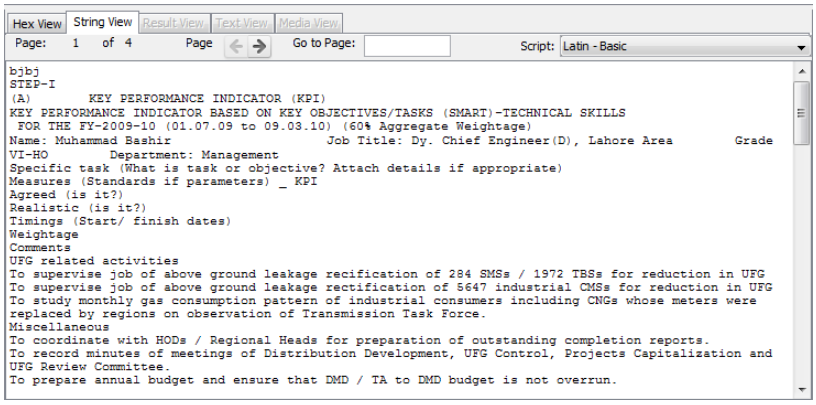


Figure 41. Example of "String Content Viewer"

Text Content Viewer: It uses the keyword search index that may have been populated during Image Ingest. If a file has text stored in the index, then this tab will be enabled, and it will be displayed to the user if a file or a result associated with a file is selected.

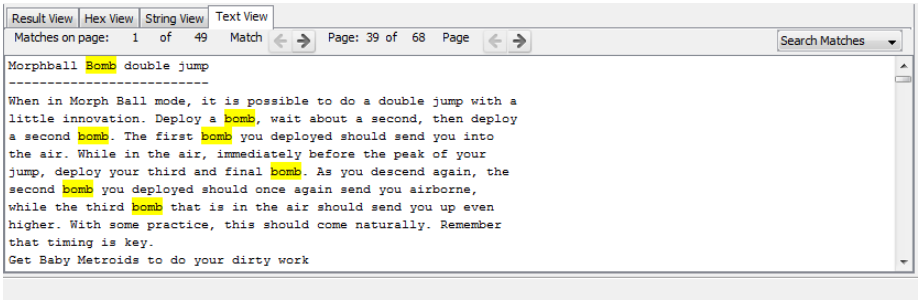


Figure 42. Example of "Text Content Viewer"

Keyword Search: It allows the user to search for keywords in the data source and it utilizes the Keyword Search Module. This module facilitates both the ingest portion of searching and also supports manual text searching after ingest has completed. It extracts text from the files being ingested and adds them to a Solr index that can then be searched.

- **Configuration:** The software relies on built-in lists that will help define regex and enable the user to search for information such as Phone Numbers, IP addresses, URLs and E-mail addresses. Although, it is important to keep in mind that enabling these general lists can result in the production of false positives due to lack of filtering.
  By the time the files are placed in the Solr index, they can be easily searched for specific keywords, regex, or keyword search lists that can contain a mixture of keywords and regex.
- **Keyword Search Configuration Dialog:** The keyword search configuration dialog has three tabs which are the Lists tab, the String Extraction tab and the General tab that are going to be discussed later.

Lists: For lists, it is possible to create new ones, import and export them. In order to create a list, the user needs to select the 'New List' button and choose a name for the new Keyword List. Once the list has been created, keywords can be added to it. Regular expressions are supported using Java Regex Syntax. Lists can be added to the keyword search ingest process; searches will happen at regular intervals as the content is added to the index.

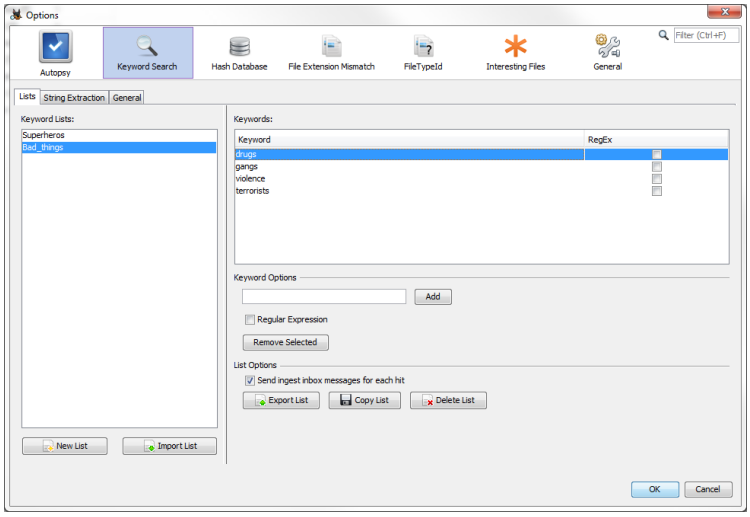


Figure 43. Lists tab in the Keyword Search Configuration Dialog

String Extraction: In this tab, the settings for extraction are defined. This will determine how the strings are extracted because their file formats are not supported. This happens with arbitrary files and chunks of unallocated space that are a representation of deleted files. Also, it is important to consider possible text encoding and script/language used when extracting string from binary files. In order to enhance the indexing performance and reduce the number of false positives, the examiner can specify a language. The default setting is to search for English strings only, encoded as either UTF8 or UTF16. However, the examiner can enable more script languages.

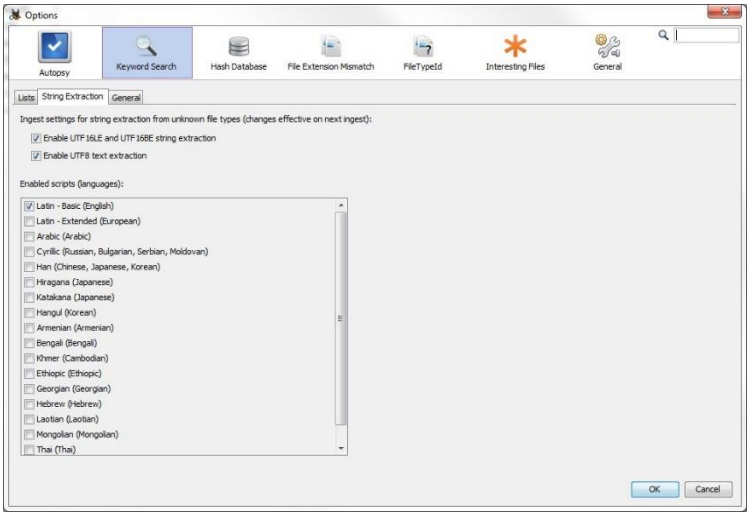


Figure 44. String Extraction tab in the Keyword Search Configuration Dialog

General: There is a possibility to configure the hash database ingest service, so it uses the NIST NSRL hash database of known files. This tab contains more advanced configuration dialog that contains an option to skip keyword indexing and search on files that have previously marked as "known" and uninteresting files. By doing so, the index size will be greatly reduced and the ingest performance improved. Another important factor is the "Results update frequency during ingest" configuration. Depending on this value, the index updates and searched being executed will be more or less frequent. A lower number of minutes results in more frequency. How- ever, the more updates the more the overall performance is affected, especially on lower-end systems, and can potentially lengthen the overall time needed for the ingest to complete. There is also the chance to avoid these periodic searches. The outcome will be an increased speed in ingest.

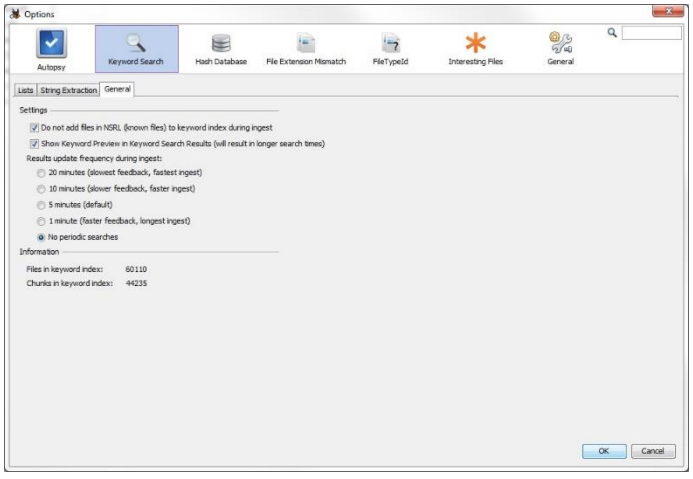


Figure 45. General tab in the Keyword Search Configuration Dialog

- **Using the Module:** Search queries can be performed at any time by one user, the only requirement is for the index to be filled with files and ready to be searched.
  In order to properly understand the needed settings, it is necessary to understand the Ingest Modules in depth. These modules analyze the data in a data source. They perform all the analysis of the files and parse their contents. Examples include hash calculation and lookup, keyword searching, and web artifact extraction. Promptly after adding a data source to a case, the examiner will be presented with a dialog that will configure the ingest modules to run on it. After the configuration is set, background processes will occur, and real-time relevant results will be returned.
  These Ingest Modules are configured to find user content fast. The ingest modules are grouped into pipelines and each file goes down the pipeline, module by module. A pipeline may have modules in the following order:

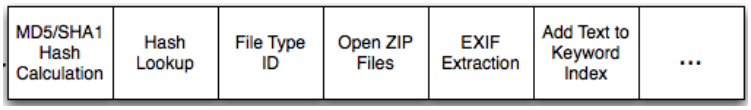


Figure 46. Modules Pipelines

Several pipelines may run simultaneously. The default configuration allows two of these pipelines to be running, but depending on the examiner's hardware, it is possible to add more pipelines.

There are two ways to start ingest modules:

1. Immediately after the data source is added.
2. By right-clicking on a data source from the tree in the main interface and choosing "Run Ingest Modules"

Once ingest is started, a bar with the currently running ingest tasks appears and these can be canceled if the user desires to do so.

Configuration: Ingest Modules

The interface shows the different ingest modules that can be enabled or disabled.

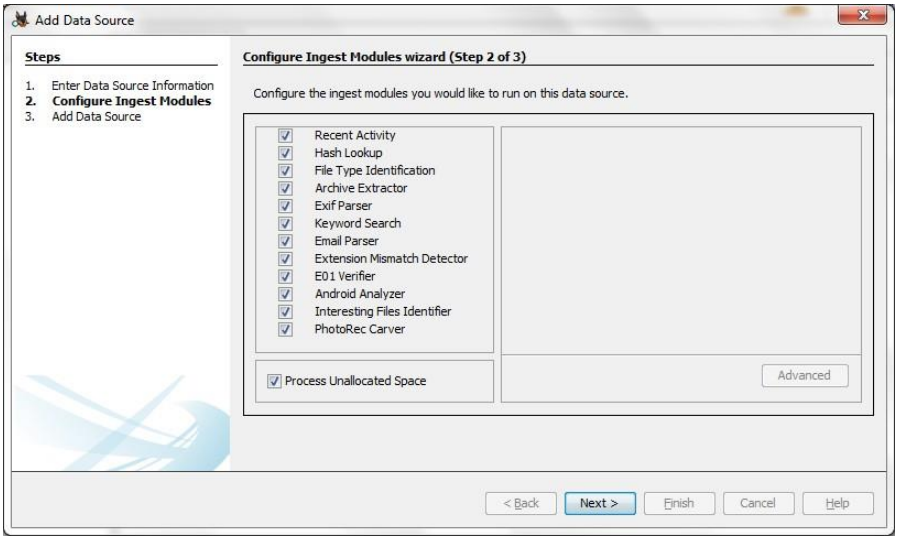


Figure 47. Ingest Modules Configuration

View Results

Ingest modules run in the background. An ingest module can provide results in a variety of ways, the software developers recommend the following specific methods:

1. If results are posted to the Blackboard, the results will be found in the "Results" area of the tree in the main interface.
2. The results can be sent to the Ingest Inbox. Therefore, each time something important is found a message will appear in this inbox.

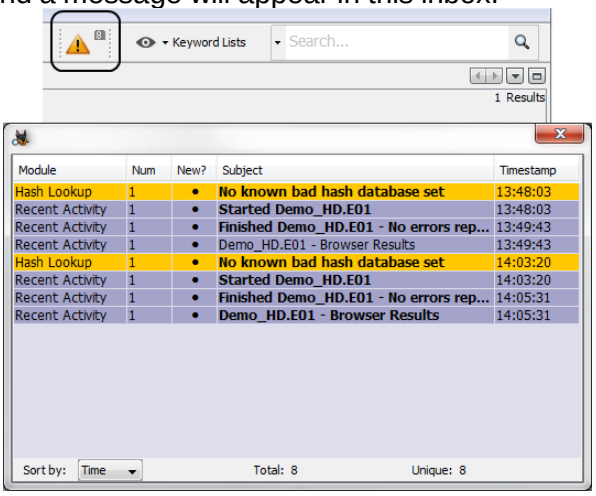


Figure 48. Ingest Box

3. If the module is a wrapper around another forensics tool, they may simply provide a link to the output of that tool. In this case, a new entry will appear in the "Reports" area of the tree.

The examiner is allowed to enable or disable the specific built-in search

expressions, Phone Numbers, IP Addresses, Email Addresses, and URLs. Using the Advanced button, it can add custom keyword groups.

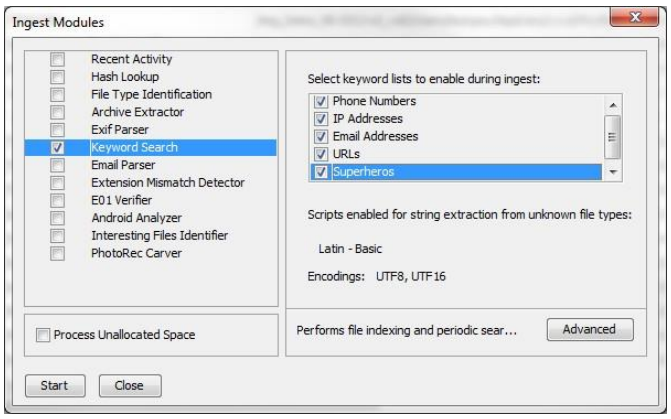


Figure 49. Ingest Settings

- **Keyword Search Bar:** It is used to search for keywords in the manual mode (outside of ingest). The existing index will be searched for matching words, phrases, lists, or regular expressions.

  Individual Keyword Search: These can quickly be searched using the search text box widget. The examiner can select "Exact Match", "Substring Match" and "Regular Expression" match.

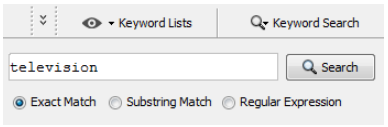


Figure 50. Individual Keyword Search

Results will be opened in a separate Results Viewer for every search executed and they will also be saved in the Directory Tree as shown in the screenshot below.

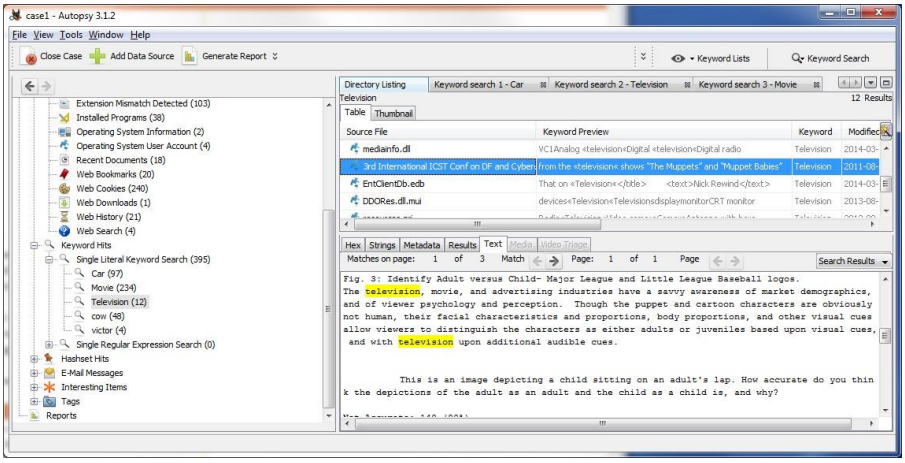


Figure 51. Individual Keyword Search Results

***Keyword List Search*:** Lists created using the Keyword Search Configuration Dialog can be manually searched by the user by pressing on the 'Keyword Lists' button, selecting the checkboxes corresponding to the lists to be searched, and pressing the 'Search' button.

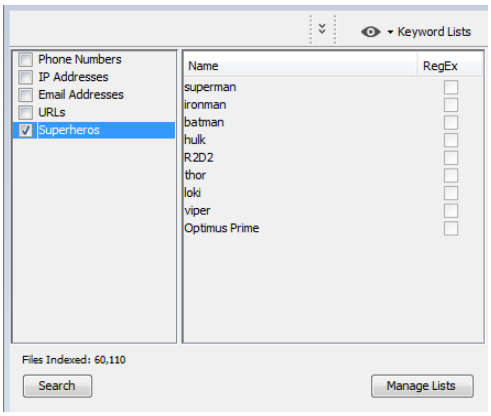


Figure 52. Keyword List Search

The results of the keyword list search are shown in the tree, as shown below.

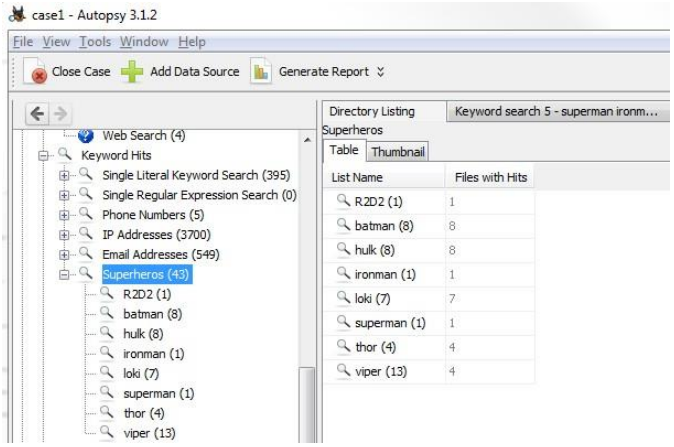


Figure 53. Keyword List Search Results

Searching during ingest: Manual search for individual keywords or regular expressions can be executed while ingest is ongoing, using the current index. However, it is possible to miss some results if the entire index has not yet been populated. Autopsy enables the search on an incomplete index in order to retrieve some preliminary results in real-time. During the ingest, the manual search by keyword list is deactivated. A newly selected list can instead be added, and it will be searched in the background instead. Keywords and lists can be managed during ingest.

Seeing Results: The Keyword Search module will save the search results regardless of whether the search is performed by the ingest process, or manually by the user. The saved results are available in the Directory Tree in the left-hand side panel.

- **Status Area:** It will show progress bars while ingest is occurring. This visually indicates to the user what portion of the processing is already complete. The user can click on the progress bars to see further detail or to cancel ingest jobs.

PhotoRec

Operating Systems

PhotoRec runs under the following O.S.:

Table 31. Operating Systems supported by PhotoRec

Operating Systems	
DOS (32-bit x86) Microsoft Windows (32-bit x86 or 64-bit x64) Linux (32-bit x86 or 64-bit x64) Mac OS X (PowerPC or Intel) / OS X / macOS	Marvell 88F628x Linux FreeBSD/OpenBSD/NetBSD Haiku SunOS/Solaris

File Systems

Table 32. File Systems supported by PhotoRec

File Systems	
FAT NTFS exFAT ext2	ext3 ext4 HFS+

File Formats Recovered By PhotoRec

Table 33. Archive file formats supported by PhotoRec

Archive	
.7z 7-Zip archive file	**.lzh** lzh/LArc archive
.a Unix/Linux archive	**.lzo** LZO archive
.ace ACE Archive	**.par2** archive
.apk Android Package Kit	**.rar** Rar archive
.arj Archive	**.rpm** RPM package
.bkf MS Backup file	**.stu** StuffIt Archive
.bz2 bzip2 compressed data	**.tar** tar archive
.cab MS cabinet archive	**.tar.gz** compressed tar archive
.dar dar3 archive	**.vbm** Veeam Backup Metadata
.deb Debian Archive	**.wim** Windows imaging (WIM) image
.dump Dump/Restore Archive	**.xar** xar archive
.ghx Grasshopper archive	**.xz** xz Archive
.gz gzip compressed data	**.zip** zip archive

Table 34. Multimedia file formats supported by PhotoRec. Part 1

Multimedia	
.3ds max	**.bmp** BMP bitmap image
.3dm Rhino / openNURBS	**.bpg** Better Portable Graphics image
.3g2 Video for 3G mobile phone (CDMA)	**.bvr** Blue Iris DVR
.3gp Video for 3G mobile phone (GSM)	**.c4d** Cinema 4d
.abr Adobe Brush	**.caf** Core Audio Format
.acb Adobe Color Book	**.cam** Image
.ado Adobe Duotone Options	**.camrec** Camtasia Camrec
.aep After Effects	**.CATDrawing** CATIA
.afdesign afdesign	**.cda** CD Audio
.aif Apple Audio	**.cdd** Concept Draw Document
.albm HP Photosmart Photo Printing Album	**.cdl** Concept Draw Library
.all Cubase Song format	**.cdr** Corel Draw
.als Ableton Live Sets	**.cdt** Concept Draw Template
.ani Windows Animated Cursor	**.celtx** Celtx, Screenwriting & Media Pre-production file
.ape Monkey's Audio compressed format	**.che** Compucon EOS Design File
.ari ARRI Raw Video	**.comicdoc** Comic Life
.arw Sony raw image (TIFF image)	**.cpi** AVCHD Clip Information
.asf, .wma, .wmv: Advanced Streaming Format used for Audio/Video	**.cpr** Cubase Project File
.asl Adobe Layer Style	**.cr2** Canon Raw 2 picture (TIFF image)
.au Sun/NeXT audio data	**.cr3** Canon Raw v3 (MOV family)
.avi RIFF video	**.crw** Canon Raw picture
.axp Pinnacle Studio	**.csh** Adobe Custom shapes
.binvox Binvox Voxel File	**.ctg** Canon catalog
.bdm AVHCD index	**.cue** Cue sheet
.bld blender	**.dad** Micae DVR
.blend Blender	**.db** Thumbs.db

Table 35. Multimedia file formats supported by PhotoRec. Part 2

Multimedia	
.dcm Digital Imaging and Communica-	**.ipt** Autodesk Inventor part ipt or iam file
tions in Medicine (DICOM)	**.iso** CD/DVD iso image (ISO0660)
.dcr Kodak Raw picture (TIFF image)	**.it** Impulse Tracker
.djv DjVu	**.itu** iTunes
.dng Adobe Digital Negative	**.ora** Mypaint .ora
.dp Designer, a Photobook Designer Soft- ware	**.jng** JPEG Network Graphics
.dpx Cineon image file/SMTPE DPX	**.jpg** JPEG 2000
.ds2 Digital Speech Standard v2	**.jpg** JPEG picture
.dsc Nikon DSC	**.kra** Krita
.dss Digital Speech Standard	**.logic** Apple Logic Studio
.ds_store Apple Desktop Services Store	**.m2t** Blu-ray MPEG-2
.dta SPSS	**.m2ts** Blu-ray MPEG-2
.dv DIF Digital Video	**.m3u** Moving Picture Experts Group Audio Layer 3 Uniform Resource Locator
.dvi TeX DVI	**.m4p** MPEG-4 Audio
.dvr RT60	**.max** 3ds
.dwg AutoCAD	**.max** Paperport
.emf Windows Enhanced MetaFile	**.mb** Maya
.epub Electronic Publication	**.mcf** Fotobook
.ers ER Mapper Rasters	**.mfa** The Games Factory Multimedia Fu- sion Files
.exs Apple Logic	.mhbd iTunes
.fcp Final Cut Pro	**.m3u** Moving Picture Experts Group Audio Layer 3 Uniform Resource Locator
.fh10 Macromedia Freehand 10	**.m4p** MPEG-4 Audio
.fh5 Macromedia Freehand 5	**.max** 3ds
.flac Free Lossless Audio Codec	**.max** Paperport
.fla Flash Project File	**.mb** Maya
.flp Fruity Loop	.mcf Fotobook
.flv Macromedia	**.mfa** The Games Factory Multimedia Fu- sion Files
.gi Roxio Creator	**.mhbd** iTunes
.gif Graphic Interchange Format	**.mid** MIDI
.gp4 Guitar Pro 4	**.mkv** Matroska
.gp5 Guitar Pro 5	**.mlv** Magic Lantern Video
.gpx Guitar Pro 6	**.mng** Multiple-Image Network Graphics
.gsm Group Speciale Mobile GSM 06.10	**.mov** Quicktime Movie
.heic High Efficiency Image File	**.mp** Maya
.icc Color profiles	**.mp3** MPEG ADTS, layer III, v1 audio
.icns Apple Icon Image	**.mp4** MPEG 4
.ico Windows Icon	**.mpg** Moving Picture Experts Group video
.idf MIDI Instruments Definition File	**.mpl** AVHCD playlist
.idx RT60	**.mpo** Multi-picture format
.iff Audio Interchange File Format	**.mrw** Minolta Raw picture
.ind InDesign File	**.mus** Finale Music Score
.ifo DVD Video manager or title set	**.mws** MetaStock
.indd Macromedia InDesign	**.nef** Nikon Raw picture (TIFF image)
.info ZoomBrowser Thumbnail info	

Table 36. Multimedia file formats supported by PhotoRec. Part 3

Multimedia	
.oci OpenCanvas Image .oci **.ogg** OGG Vorbis audio **.ogm** OGG audio **.ogv** Ogg data, Theora video **.orf** Olympus Raw Format picture **.pbm** Portable Bitmap **.pct** Macintosh Picture **.pcx** PCX file format **.psb** Adobe Photoshop Image **.pef** Pentax Raw picture (TIFF image) **.pgm** Portable GrayMap **.png** Portable Network Graphics **.pnm** Portable anymap **.ppm** Portable PixMap **.prproj** Adobe Premiere project **.psd** Adobe Photoshop Image **.psf** Print Shop File **.psp** Paint Shop Pro Image File **.ptb** PowerTab **.pts** PTGui, panoramic stitching software **.pvp** Php Video Pro **.qcp** The QCP File Format and Media Types for Speech Data **.qkt** Apple QuickTake 100 **.qxd** QuarkXpress Document **.qxp** QuarkXpress Document **.r3d** RED r3d camera **.raf** Raw Fujifilm picture **.ram** Real Media **.ra** Real Audio **.raw** Contax picture, Panasonic/Leica picture **.rdc** Rollei picture **.rm** Real Media **.rns** Reason **.rns** Reason Audio File **.rpp** Reaper Project **.rw2** Panasonic Raw 2 **.rx2** Zotope RX 2, Audio Repair Software file **.ses** Cool Edit/Adobe Audition session	**.shn** Shorten audio file **.sib** Sibelius **.sit** Mikron **.skd** AutoSketch drawing **.sketch** Vector graphics file created by Sketch **.smil** Synchronized Multimedia Integration Language **.spss** SPSS **.sr2** Sony Raw picture (TIFF image) **.svg** Scalable Vector Graphics **.swc** Macromedia Compressed Flash **.swf** MacroMedia Flash (Compiled) **.tg** Tux Guitar 1.2 **.tif** Tag Image File Format **.TiVo** video record **.tod** Blu-ray MPEG-2 **.tpl** Adobe Tool Preset **.ts** MPEG-2 Transport Stream **.vdj** VirtualDJ **.wav** RIFF audio **.wdp** JPEG XR **.webm** Matroska **.webp** WebP Image Format **.wee** weecast **.wmf** Windows Metafile **.wnk** Wink screen capture **.wpb** OpenCanvas files **.wpl** Windows Play List **.wtv** Windows Media Center TV **.wv** WavPack, Hybrid Lossless Wavefile Compressor **.x3f** Sigma/Foveon X3 raw picture **.x3i** Sigma/Foveon X3 raw picture **.xcf** GIMP XCF File **.xd** Adobe xd **.xm** FastTrackerII Extended Module **.xmp** Adobe's Extensible Metadata Platform **.xrns** Extended Renoise song file **.xv** XV thumbnail image **.zcode** Zortrax 3D printing

Table 37. Office file formats supported by PhotoRec

Office	
.accdb Microsoft Access database	**.qpw** Quattro Pro spreadsheet
.ai Adobe Illustrator (Part of PDF file family)	**.rtf** Rich Text Format
.apr Lotus Approach	**.sda** StarDraw (OLE document)
.csv Comma separated values	**.sdc** StarCalc (OLE document)
.cwk AppleWorks	**.sdd** StarImpress (OLE document)
.doc Microsoft Word (OLE document)	**.sdw** StarWriter (OLE document)
.docx Microsoft Office "Open" XML (ZIP Archive)	**.slk** Sylk, Multiplan Symbolic Link Inter-change
.et Microsoft Excel	**.sav** SPSS (Statistical Package for the So- cial Sciences) saved data
.fb2 FictionBook	**.snt** Windows Sticky Notes
.fods OpenDocument Flat XML Spread-sheet	**.sxc** OpenOffice Spreadsheet (ZIP archive)
.fp7 File Maker Pro 7	**.sxd** OpenOffice Drawing (ZIP archive)
.fp12 File Maker Pro 12	**.sxi** OpenOffice Presentation (ZIP archive)
.gnucash GnuCash,	**.sxw** OpenOffice Text Document (ZIP archive)
.kmy KMyMoney (gz file family)	**.tex** LaTeX (Text file family)
.lyx LyX	**.txt** Text file
.mdb Microsoft Access database (Ole document)	**.vsd** Visio document (OLE document)
.njx NJStar	**.vsdx** Microsoft Visio 2010+
.odg OpenDocument Graphics (ZIP Archive)	**.wpd** Corel Documents
.odp OpenDocument Presentation (ZIP Archive)	**.wps** Microsoft Works
.ods OpenDocument Spreadsheet (ZIP Archive)	**.xlr** Microsoft Works Spreadsheet or Chart
.odt OpenDocument Text (ZIP Archive)	**.xls** Microsoft Excel (OLE document)
.one Microsoft OneNote	**.xlsx** Microsoft Office "Open" XML
.pages iWork	**.wdb** Microsoft Works Database
.pap Papyrus word file	**.wk4** Lotus 1-2-3
.ppt PowerPoint presentation	**.wks** Lotus 1-2-3
.pptx Microsoft Office "Open" XML (ZIP Archive)	**.pub** Microsoft Publisher (OLE docu-ment)
.qbb Quickbooks Backup	**.qbw** Quickbooks - Company File

Table 38. Other file formats supported by PhotoRec. Part 1

Others	
.1cd Russian Finance 1C:Enterprise 8	**.dgn** MicroStation CAD file format
.ab Mac Address Book	**.dif** Lotus Data Interchange Format
.adr Opera Hotlist	**.dim** SunPCI Disk Image
.agn Autogen	**.diskimage** SunPCI Disk Image
.ahn Ahnenblatt	**.dll** Microsoft Dynamic Link Library
.amb Licom AlphaCAM	**.dmp** Oracle Dump
.amd AlphaCAM	**.drw** Pro/ENGINEER Drawing
.amr Adaptive Multi-Rate	**.dsa** SSH DSA private key
.amt AlphaCAM	**.dst** Tajima
.apa APA Style Helper	**.dxf** Drawing Interchange File
.apple AppleSingle/AppleDouble	**.e01** Encase
.asm Pro/ENGINEER Assembly	**.ecr** Encrypted file by eCryptfs
.asp ASP script	**.eCryptfs** Encrypted file by eCryptfs
.atd Agelong Tree Database/Abs0luteDatabase	**.edb** Exchange Database
.atd AlphaCAM	**.elf** Executable and Linking Format
.att AlphaCAM	**.emb** Wilcom ES Software
.axx AxCrypt	**.emka** EMKA IOX (isolated organ exper- iments) data
.bac Bacula backup	**.emlx** Mac OSX mail format
.bai SAM/BAM and related high-throughput sequencing file formats	**.eps** Encasulated PostScript
.bam SAM/BAM and related high-throughput sequencing file formats	**.ess** Skyrim Savegame
.bat Dos/Windows Batch	**.evt** Windows registry header detection and Event Log
.bgz SAM/BAM and related high-throughput sequencing file formats	**.evtx** Microsoft Event Log
.bim Broadcast Interface Module	**.exe** Microsoft executable (PE)
.c	**.fbf** SymBackup
.chm Microsoft Windows HtmlHelp Data	**.fbk** Microsoft Dynamics NAV (MS Nav- ision)
.class Java Class	**.fcs** Flow Cytometry Standard 3.0
.cls Microsoft VB	**.fdb** Microsoft Dynamics NAV (MS Nav- ision)
.cm Comic Life	**.fds** fwNES Disk Image (with header)
.compress MS compress file (SZDD)	**.f** Fortran
.cow Qemu Image	**.fh1** Macromedia Freehand 10
.cp_ MS compress file (SZDD)	**.fit** Flexible & Interoperable Data Transfer / Garmin track file
.csi SAM/BAM and related high-throughput sequencing file formats	**.fits** NASA Flexible Image Transport Sys- tem
.d2s Diablo II	**.fm** Football Manager
.dat Internet Explorer index.dat- MAJ	**.fob** Microsoft Dynamics NAV (MS Nav- ision)
.dbf DBase 3 (prone to false positive)	**.fos** Fallout 4 Savegame
.dbn DriftBox	**.fp5** File Maker Pro
.dbx Outlook Express	**.freeway** Freeway 5 Pro
.dc TSCe Survey Controller DC v10.0	**.frm** MySQL table definition
.ddf Didson Data File (v3 and v4)	**.frm** Pro/ENGINEER Drawing Form
.dex Dalvik	**.fst** QuickBook

Table 39. Other file formats supported by PhotoRec. Part 2

Others	
.fs Zope data8	**.jsp** JSP script
.fwd FRWD Sports Computer	**.kdb** KeePassX
.gam Games Factory	**.kdbx** KeePassX
.gcs GCstart (personal collections man- ager)	**.key** Synology AES key
.gct XFI Electronic Fuel Injection Systems	**.kmz** Zipped Keyhole Markup Language (KML) used by Google Earth
.gho Ghost image file	**.ldf** Microsoft SQL Server Log Data File
.gm6 Game Maker 6.0-6.1	**.ldif** LDAP Data Interchange Format
.gm81 Game Maker 8.1	**.lit** Microsoft ITOL/ITLS
.gmd Game Maker 4.3-5.3A	**.lnk** Microsoft Windows Link
.gmk Game Maker 7.0-8.0	**.lso** Logic Platinum File
.gp2 Gobe Productive Document	**.luks** LUKS encrypted file
.gpg Partial support for GPG/OpenPGP file recovery	**.lwo** 3d model
.gsb Grisbi - Personal Finance Manager XML data	**.lxo** lxo/lwo 3d model
.h C header	**.ly** LilyPond
.hdf Hierarchical Data Format 4	**.mat** Mathlab
.hdr ENVI	**.mcd** VectorWorks
.hds Parallels disk image	**.mdf** Microsoft SQL Server Master Database File
.hm HyperMesh, structural analysis soft- ware	**.mdl** Mathlab Model
.hr9 Heredis - Genealogy	**.mem** Mnemosyne Data Base
.html.gz compressed HTML	**.mfg** Pro/ENGINEER Manufacturing
.html HTML	**.mig** Windows Migration Backup
.http HTTP Cache	**.mk5** Custom CAD-CAM
.ibd InnoDB database file	**.mmap** MindManager
.ics vcalendar	**.mny** MS Money (Recovered as .mdb MS Access Database)
.imb Incredimail	**.mobi** Mobi e-book
.img Filevault	**.msa** Mensura
.imm Incredimail	**.msf** Mozilla "mork database"
.inf Windows Autorun	**.msg** Outlook
.ini Windows .ini	**.mxf** Material Exchange Format
.jad Java Application Descriptor	**.MYI** MySQL MISAM compressed data
.jar Java Archive	**.myo** Mind Your Own Business
.jks Java Keystore	**.nd2** NIS-Elements
.jnb SigmaPlot	**.nds** Nintendo DS Game ROM Image
.jp2 sample	**.nes** iNES/iNES 2.0 ROM image
.json JavaScript Object Notation	**.nk2** Outlook Nickfile
.jsonlz4 Mozilla bookmarks	**.notebook** SMART Notebook
.nsf Lotus Notes	**.pds** Reson - Sonar Data
.p65 Page Maker	**.pf** Windows prefetch file
.paf Personal Ancestral File	**.pfx** files holding PKCS 12 keys
.pcap tcpdump capture file	**.pgp** OpenPGP/GnuPG encrypted data
.pcb PCB Wizard	**.php** PHP script
.pcp pcap capture low-endian header	**.pli** Mac OS X property list
.pdb Protein Data Bank data	**.plist** Apple plist
.pdf Portable Document Format	**.pl** Perl script

Table 40. Other file formats supported by PhotoRec. Part 3

Others	
.plt Gerber Graphix Advantage	**.sql** MySQL, phpMyAdmin, PostgreSQL dump
.pm Perl module	**.sqm** Windows Live Messenger Log File
.ppk Putty Public Key	**.steuer2014** Steuer 2014
.prc PalmOS application	**.steuer2015** Steuer 2015
.prd Paessler PRTGs	**.stl** Stereolithography CAD
.priv PGP private key	**.stp** Standard for the Exchange of Product model data
.prt Pro/ENGINEER Model	**.studio** Silhouette Cameo cutting machine
.psmodel Delcam PowerSHAPE	**.tax** Turbo Tax
.ps PostScript document	**.tcw** TurboCAD for Windows
.pst Outlook	**.tib** Acronis True Imag
.ptf Pro Tools session File	**.ticket.bin** DINO
.ptx Pro Tools session File	**.torrent** Torrent data filel
.pub SSH DSA/RSA public key	**.tph** Pro/ENGINEER ToolPath
.pub PGP public key	**.ttd** TinyTag Data
.pyc Python Compiled Script	**.ttf** TrueType Font
.py Python script	**.tz** Timezone info
.pzf GraphPrism 4	**.url** Windows URL / Internet Shortcut
.pzh Presto	**.v2i** v2i backup
.qbb Quickbooks	**.vault** McAfee Anti-Theft/FileVault
.qbmb Quickbooks	**.vb** Microsoft Visual Basic
.qbw Quickbooks	**.vcf** VCard
.qdf-backup qdf-backup	**.vdi** Virtual desktop infrastructure 1.1
.qdf Quicken	**.veg** Sony Vegas
.qgs Quantum GIS	**.vfb** FontLab
.rb Ruby	**.vib** Veeam Incremental Backup
.RData R Data	**.wallet** Armory bitcoin wallet
.reg Windows registry config file	**.vmdk** Vmware
.res Microsoft Visual Studio Resource	**.vmg** Nokia Text Message
.rfp Roboform	**.wab** Windows Address Book
.rlv Revelation password	**.wim** Windows imaging (WIM) image
.rsa SSH RSA private key	**.win** Opera preferences
.rvt Revit	**.wld** Terraria world
.save Assassin's Creed II backup	**.woff** Web Open Font Format
.schematic Minecraft Schematic File	**.x4a,.x4g,.x4p, .x4s** Yamaha-YSFC
.sgcta Ciel	**.xfi** XFI Electronic Fuel Injection Systems
.sh3d Sweet Home 3Ds	**.xml.gz** compressed XML
.sh Shell script	**.xml** XML
.skp SketchUp	**.xoj** Xournal
.sla Scribuse	**.xpi** Mozilla application
.sldprt SolidWorkse	**.xpt** Mozilla XPCOM Type Library
.sld SolidWorks	**.xsv** XBOX GTA San Andreas Save File
.snag Snagit	**.z2d** ZeroCad
.sp3 Sisporto SP3/SPM	**.zpr** Zbrush
.sparseimage Filevault	**.spf** ShadowProtect
.spe WinSpec	**.sqlite** SQLite databases

FTK Imager

Installation

Locally

This kind of installation should be executed when there is an intention to attach evidence hardware to the computer for previewing and imaging evidence.

1. Browse to the FTK Imager setup file, either from an installation disc or from the saved file downloaded from http://accessdata.com/support/adownloads.
2. Under FTK Imager, select the version desired. Click Download.
3. Click Save File.
4. Browse to the location where it is desired to save the install file, and click Save.
5. When the download is complete, browse to the location where it was saved.
6. Execute the setup file by double-clicking it.
7. On the Welcome screen, click Next.
8. Read and accept the License Agreement, then click Next.
9. Do one of the following:
- Accept the default installation location.
- Browse to a different destination folder.
10. Click Next.
11. In the Ready to Install screen, click Next.
12. Do one of the following:
- Mark the Launch AccessData FTK Imager box to force Imager to run immediately after the install is complete.
- Leave the box unmarked to run the newly installed program later.
13. Click Finish to complete the installation and close the wizard.

Portable Device

There are two ways to use Imager on a portable device:

- Copy the FTK Imager Lite files directly to the device, avoiding installing it to a local computer first.
  Unzip the downloaded files to the portable drive and execute the file from there. The FTK Imager Lite program has fewer files (only the essentials) and does not require a separate installation, although it is necessary to unzip the downloaded file to extract its contents into a folder before use.
- Run the installation on a local computer, then copy the FTK Imager folder from the [Drive]:\Program Files\AccessData\FTK Imager to the thumb drive or other portable device.

Once the FTK Imager program files are saved to the portable media, that media can be connected to any computer running a Windows OS, and the program file, FTK Imager.exe can be executed from the portable media device.

With either method, it is necessary to make a target drive available for saving the imaged data, and a reliable write-blocker must still be used.

Running FTK Imager

FTK Imager can be run in a variety of ways:

- Double-click on the desktop icon.
- Execute the FTK Imager.exe file from a thumb drive.
- Click Start > Run > Browse. Browse to and select FTK Imager.exe from the location it was installed to and add a command-line switch as discussed below.

Command-Line Options

FTK Imager supports three command-line options:

- `/CreateDirListing`: Creates a directory listing file in the folder where FTK Imager.exe is run from.
- `/VerifyImage`: Verifies an image when the user specifies the image path and file- name.
- `/EnableDebugLog`: Enables logging to the FTKImageDebug.log file created in the folder the user runs FTK Imager.exe from.

Features

According to its documentation, these are the following procedures an examiner can carry through with FTK Imager:

- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, and DVDs, entire folders, or individual files from various places within the media.
- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs
- Preview the contents of forensic images stored on the local machine or a network drive
- Mount an image for a read-only view that leverages Windows Explorer to see the content of the image exactly as the user saw it on the original drive.
- Export files and folders from forensic images.
- See and recover files that have been deleted from the Recycle Bin but have not yet been overwritten on the drive.
- Create hashes of files using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).
- Generate hash reports for regular files and disk images (including files inside disk images) that the user can later use as a benchmark to prove the integrity of the

case evidence. When a full drive is imaged, a hash generated by FTK Imager can be used to verify that the image hash and the drive hash match after the image is created and that the image has remained unchanged since acquisition.

User Interface

Menu Bar

- **File:** provides access to all the features that can be used from the Toolbar.

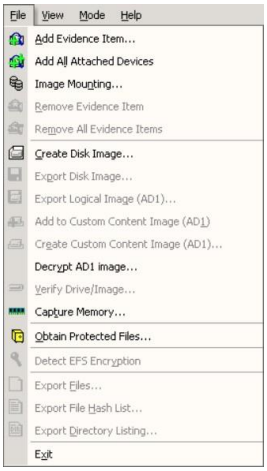


Figure 54. Screenshot of options available in the File menu

- **View:** allows the customization of the appearance of the software interface, this also includes showing or hiding panes and control bars. The panes that appear in the following screenshot are going to be discussed later.

Figure 55. Screenshot of options available in the View menu

- **Mode:** allows the selection of the preview mode of the Viewer.

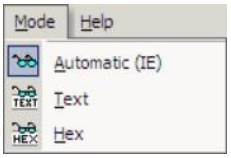


Figure 56. Screenshot of options available in the Mode menu

FTK Imager offers three modes for previewing electronic data: Automatic mode, Text mode, and Hex mode.

- **Automatic Mode:** Automatic mode automatically chooses the best method for previewing a file's contents, according to the file type. For example:
  - Web pages, Web-related graphics (JPEGs and GIFs), and any other media types for which Internet Explorer plug-ins have been installed are displayed by an embedded version of Internet Explorer in the Viewer.
  - Text files are displayed in the Viewer as ASCII or Unicode characters.
  - File types that cannot be viewed in Internet Explorer are displayed outside of FTK Imager in their native application provided those applications are installed locally, and the appropriate file associations have been configured in Windows.
  - File types that cannot be viewed in Internet Explorer and that do not have a known native viewer are displayed by default in Hexadecimal Mode in the Viewer.
- **Text Mode:** Text mode allows the preview of a file's contents as ASCII or Unicode characters, even if the file is not a text file. This mode can be useful for viewing text and binary data that is not visible when a file is viewed in its native application.
- **Hex Mode:** Hex mode allows the user to view every byte of data in a file as hexadecimal code. It is possible to use the Hex Value Interpreter to interpret hexadecimal values as decimal integers and possible time and date values.

- **Help:** provides access to the FTK Imager User Guide, and to information about the program version and so forth.

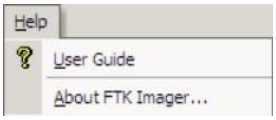


Figure 57. Screenshot of options available in the Help menu

Toolbar

The Toolbar contains all the tools, functions, or features, that can be accessed from the File menu, except Exit. In the Figure 58 the different buttons and descriptions are specified in order to provide information about each feature present in the software.

View Panes

- **Evidence Tree Pane:** this pane displays the added evidence items in a hierarchical tree. At the root of the tree are the selected evidence sources. Listed below each source are the folders and files it contains. By clicking the plus sign (+) or minus sign (-) next to a source it is possible to expand the view to display its subfolders or hide its contents.
- **File List Pane:** when an object in the Evidence Tree is selected the contents contained in it are displayed in this pane. The content displayed changes as the user changes the selection.
- **Combination Pane:** displays a variety of information about the object currently selected in either the Evidence Tree or the File List.
  - **Properties:** includes information such as object type, size, location on the storage media, flags, and time stamps.
  - **Hex Value Interpreter:** converts hexadecimal values selected in the Viewer into decimal integers and possible time and date values.
  - **Custom Content Sources:** it displays a list of the times when the user adds an item to be included in a Custom Content image.

File Systems and Drive Image Formats

In this subsection, the file systems and image formats that AD Imager recognizes are listed in the following tables.

Table 41. File Systems supported by FTK Imager

File Systems		
FAT12,FAT16,FAT32	NTFS	HFS+
Ext2FS, Ext3FS, Ext4FS	HFS	CDFS
ReiserFS3	VXFS	exFAT

Button	Description
	Add Evidence Item
	Add All Attached Devices
	Image Mounting. Opens the Map Image to Drive dialog.
	Remove Evidence Item
	Remove All Evidence Items
	Create Disk Image
	Export Disk Image
	Export Logical Image (AD1)
	Add to Custom Content Image (AD1)
	Create Custom Content Image (AD1)
	Verify Drive/Image
	Capture Memory
	MetaCarve (Deep Scan)
	Obtain Protected Files
	Detect EFS Encryption
	Export Files
	Export File Hash List
	Export Directory Listing
	Choose IE, text, or hex viewer automatically
	View files in plain text
	View files in hex format
	Open FTK Imager User Guide
	Show or Hide Panels. Choose to show or hide the *Toolbar*, *Evidence Tree*, *File List*, *Properties*, *Hex Value Interpreter*, and/or *Custom Content Sources Panes*.

Figure 58. Features in the Toolbar

Table 42. Whole Disk Encrypted supported by FTK Imager

Whole Disk Encrypted			
EPGP Credant SafeBoot	Utimaco Guardian Edge EFS	JFS VMware UFS1	UFS2 LVM LVM2

Table 43. Hard Disk Image Formats supported by FTK Imager

Hard Disk Image Formats		
Encase, including 6.12 Safeback 2.0 and under Linux DD Ghost (forensic images only)	SnapBack Expert Witness ICS	Advanced Forensics Format (AFF) AccessData Logical Image (AD1) SMART

Table 44. CD and DVD Image Formats supported by FTK Imager

CD and DVD Image Formats			
Alcohol(*.mds) PlexTools(*.pxi) Nero(*.nrg) ISO Virtual CD(*.vc4) VCD DVD+MRW DVD-RW DVD+RW Dual Layer BD-R SRM-POW BD-R SRM HD DVD-R SVCD	soBuster CUE CloneCD(*.ccd) Roxio(*.cif) Pinnacle(*.pdi) CD-RW, CD-ROM DVCD DVD-VFR DVD-VR BD-R DL CloneCD(*.ccd) D DVD-RW DL HD DVD	BD-RE DL BD-R SRM+POW DVD-R Dual Layer VD-R DVD+RW Virtual CD (*.vc4) HD DVD-RAM BDAV HD DVD-R DL BD-RE DVD+R CD-MRW, HD DVD-RW	BD-R DVD+VRW DVD-VM DVD-ROM SACD CD-R Pinnacle(*.pdi) BD-R RRM BD-ROM DVD+R Dual Layer DVD+VR CD-ROM XA DVD-RAM,

Volatility

Operating Systems

Windows

Table 45. Windows memory images supported by Volatility

Windows memory images supported	
32-bit Windows XP Service Pack 2 and 3	64-bit Windows Vista Service Pack 0, 1, 2
32-bit Windows 2003 Server Service Pack 0, 1, 2	64-bit Windows 2008 Server Service Pack 1 and 2
32-bit Windows Vista Service Pack 0, 1, 2	64-bit Windows 2008 R2 Server Service Pack 0 and 1
32-bit Windows 2008Server Service Pack 1,2	64-bit Windows 7 Service Pack 0 and 1
32-bit Windows 7 Service Pack 0, 1	64-bit Windows 8, 8.1, and 8.1 Update 1 64-bit Windows Server 2012 and 2012 R2
32-bit Windows 8, 8.1, and 8.1 Update 1 32-bit Windows 10 (initial support)	64-bit Windows 10 (including at least 10.0.18362) 64-bit Windows Server 2016)
64-bit Windows XP Service Pack 1 and 2	
64-bit Windows 2003 Server Service Pack 1 and 2	

Mac OS X

Table 46. Mac OS X memory images supported by Volatility

Mac OS X memory images supported	
32-bit 10.5.x Leopard	64-bit 10.10.x Yosemite
32-bit 10.6.x Snow Leopard	64-bit 10.11.x El Capitan
64-bit 10.6.x Snow Leopard	64-bit 10.12.x Sierra
32-bit 10.7.x Lion	64-bit 10.12.x High Sierra
64-bit 10.7.x Lion	64-bit 10.14.x Mojave
64-bit 10.8.x Mountain Lion	64-bit 10.15.x Catalina
64-bit 10.9.x Mavericks	

Linux

Table 47. Linux memory images supported by Volatility

Linux memory images supported
32/64-bit Linux kernels 2.6.11 to 5.5
OpenSuSE, Ubuntu, Debian, CentOS, Fedora, Mandriva, etc

Formats

Table 48. Memory Format Support for Volatility

Memory Format Support	
Raw linear sample (dd)	LiME format
Hibernation file (Windows 7 and earlier)	Mach-O file format
Crash dump file	QEMU virtual machine dumps
VirtualBox ELF64 core dump	Firewire
EWF format (E01)	HPAK (FDPro)
VMware saved state and snapshot files	

Network Working Group
Request for Comments: 3227
BCP: 55
Category: Best Current Practice

D. Brezinski
In-Q-Tel
T. Killalea
neart.org

February 2002

Guidelines for Evidence Collection and Archiving

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Abstract

A "security incident" as defined in the "Internet Security Glossary", RFC 2828, is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

Table of Contents

1 Introduction

A "security incident" as defined in [RFC2828] is a security-relevant system event in which the system's security policy is disobeyed or otherwise breached. The purpose of this document is to provide System Administrators with guidelines on the collection and archiving of evidence relevant to such a security incident. It's not our intention to insist that all System Administrators rigidly follow these guidelines every time they have a security incident. Rather, we want to provide guidance on what they should do if they elect to collect and protect information relating to an intrusion.

Such collection represents a considerable effort on the part of the System Administrator. Great progress has been made in recent years to speed up the re-installation of the Operating System and to facilitate the reversion of a system to a 'known' state, thus making the 'easy option' even more attractive. Meanwhile little has been done to provide easy ways of archiving evidence (the difficult option). Further, increasing disk and memory capacities and the more widespread use of stealth and cover-your-tracks tactics by attackers have exacerbated the problem.

If evidence collection is done correctly, it is much more useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution.

You should use these guidelines as a basis for formulating your site's evidence collection procedures, and should incorporate your site's procedures into your Incident Handling documentation. The guidelines in this document may not be appropriate under all jurisdictions. Once you've formulated your site's evidence collection procedures, you should have law enforcement for your jurisdiction confirm that they're adequate.

1.1 Conventions Used in this Document

The key words "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119].

2 Guiding Principles during Evidence Collection

- Adhere to your site's Security Policy and engage the appropriate Incident Handling and Law Enforcement personnel.
- Capture as accurate a picture of the system as possible.
- Keep detailed notes. These should include dates and times. If possible generate an automatic transcript. (e.g., On Unix systems the 'script' program can be used, however the output file it generates should not be to media that is part of the evidence). Notes and print-outs should be signed and dated.
- Note the difference between the system clock and UTC. For each timestamp provided, indicate whether UTC or local time is used.
- Be prepared to testify (perhaps years later) outlining all actions you took and at what times. Detailed notes will be vital.
- Minimise changes to the data as you are collecting it. This is not limited to content changes; you should avoid updating file or directory access times.
- Remove external avenues for change.
- When confronted with a choice between collection and analysis you should do collection first and analysis later.
- Though it hardly needs stating, your procedures should be implementable. As with any aspect of an incident response policy, procedures should be tested to ensure feasibility, particularly in a crisis. If possible procedures should be automated for reasons of speed and accuracy. Be methodical.
- For each device, a methodical approach should be adopted which follows the guidelines laid down in your collection procedure. Speed will often be critical so where there are a number of devices requiring examination it may be appropriate to spread the work among your team to collect the evidence in parallel. However on a single given system collection should be done step by step.
- Proceed from the volatile to the less volatile (see the Order of Volatility below).

- You should make a bit-level copy of the system's media. If you wish to do forensics analysis you should make a bit-level copy of your evidence copy for that purpose, as your analysis will almost certainly alter file access times. Avoid doing forensics on the evidence copy.

2.1 Order of Volatility

When collecting evidence you should proceed from the volatile to the less volatile. Here is an example order of volatility for a typical system.

- registers, cache
- routing table, arp cache, process table, kernel statistics, memory
- temporary file systems
- disk
- remote logging and monitoring data that is relevant to the system in question
- physical configuration, network topology
- archival media

2.2 Things to avoid

It's all too easy to destroy evidence, however inadvertently.

- Don't shutdown until you've completed evidence collection. Much evidence may be lost and the attacker may have altered the startup/shutdown scripts/services to destroy evidence.
- Don't trust the programs on the system. Run your evidence gathering programs from appropriately protected media (see below).
- Don't run programs that modify the access time of all files on the system (e.g., 'tar' or 'xcopy').

- When removing external avenues for change note that simply disconnecting or filtering from the network may trigger "deadman switches" that detect when they're off the net and wipe evidence.

2.3 Privacy Considerations

- Respect the privacy rules and guidelines of your company and your legal jurisdiction. In particular, make sure no information collected along with the evidence you are searching for is available to anyone who would not normally have access to this information. This includes access to log files (which may reveal patterns of user behaviour) as well as personal data files.

- Do not intrude on people's privacy without strong justification. In particular, do not collect information from areas you do not normally have reason to access (such as personal file stores) unless you have sufficient indication that there is a real incident.

- Make sure you have the backing of your company's established procedures in taking the steps you do to collect evidence of an incident.

2.4 Legal Considerations

Computer evidence needs to be

- Admissible: It must conform to certain legal rules before it can be put before a court.

- Authentic: It must be possible to positively tie evidentiary material to the incident.

- Complete: It must tell the whole story and not just a particular perspective.

- Reliable: There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.

- Believable: It must be readily believable and understandable by a court.

3 The Collection Procedure

Your collection procedures should be as detailed as possible. As is the case with your overall Incident Handling procedures, they should be unambiguous, and should minimise the amount of decision-making needed during the collection process.

3.1 Transparency

The methods used to collect evidence should be transparent and reproducible. You should be prepared to reproduce precisely the methods you used, and have those methods tested by independent experts.

3.2 Collection Steps

- Where is the evidence? List what systems were involved in the incident and from which evidence will be collected.
- Establish what is likely to be relevant and admissible. When in doubt err on the side of collecting too much rather than not enough.
- For each system, obtain the relevant order of volatility.
- Remove external avenues for change.
- Following the order of volatility, collect the evidence with tools as discussed in Section 5.
- Record the extent of the system's clock drift.
- Question what else may be evidence as you work through the collection steps.
- Document each step.
- Don't forget the people involved. Make notes of who was there and what were they doing, what they observed and how they reacted.

Where feasible you should consider generating checksums and cryptographically signing the collected evidence, as this may make it easier to preserve a strong chain of evidence. In doing so you must not alter the evidence.

4 The Archiving Procedure

Evidence must be strictly secured. In addition, the Chain of Custody needs to be clearly documented.

4.1 Chain of Custody

You should be able to clearly describe how the evidence was found, how it was handled and everything that happened to it.

The following need to be documented

- Where, when, and by whom was the evidence discovered and collected.
- Where, when and by whom was the evidence handled or examined.
- Who had custody of the evidence, during what period. How was it stored.
- When the evidence changed custody, when and how did the transfer occur (include shipping numbers, etc.).

4.2 Where and how to Archive

If possible commonly used media (rather than some obscure storage media) should be used for archiving.

Access to evidence should be extremely restricted, and should be clearly documented. It should be possible to detect unauthorised access.

5 Tools you'll need

You should have the programs you need to do evidence collection and forensics on read-only media (e.g., a CD). You should have prepared such a set of tools for each of the Operating Systems that you manage in advance of having to use it.

Your set of tools should include the following:

- a program for examining processes (e.g., 'ps').
- programs for examining system state (e.g., 'showrev', 'ifconfig', 'netstat', 'arp').
- a program for doing bit-to-bit copies (e.g., 'dd', 'SafeBack').

- programs for generating checksums and signatures (e.g., 'shalsum', a checksum-enabled 'dd', 'SafeBack', 'pgp').

- programs for generating core images and for examining them (e.g., 'gcore', 'gdb').

- scripts to automate evidence collection (e.g., The Coroner's Toolkit [FAR1999]).

The programs in your set of tools should be statically linked, and should not require the use of any libraries other than those on the read-only media. Even then, since modern rootkits may be installed through loadable kernel modules, you should consider that your tools might not be giving you a full picture of the system.

You should be prepared to testify to the authenticity and reliability of the tools that you use.

6 References

[FAR1999] Farmer, D., and W Venema, "Computer Forensics Analysis Class Handouts", http://www.fish.com/forensics/

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September 1997.

[RFC2350] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", FYI 8, RFC 2350, June 1998.

[RFC2828] Shirey, R., "Internet Security Glossary", FYI 36, RFC 2828, May 2000.

7 Acknowledgements

We gratefully acknowledge the constructive comments received from Harald Alvestrand, Byron Collie, Barbara Y. Fraser, Gordon Lennox, Andrew Rees, Steve Romig and Floyd Short.

8 Security Considerations

This entire document discuses security issues.

9 Authors' Addresses

Dominique Brezinski
In-Q-Tel
1000 Wilson Blvd., Ste. 2900
Arlington, VA 22209
USA

EMail: dbrezinski@In-Q-Tel.org

Tom Killalea
Lisi/n na Bro/n
Be/al A/tha na Muice
Co. Mhaigh Eo
IRELAND

Phone: +1 206 266-2196
EMail: tomk@neart.org

10. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

TALON ULTIMATE

A powerful forensic imaging solution with exceptional performance, features & reliability

- **Extremely fast forensic imaging at over 40GB/min**
- **Image to or from a network repository**
- **Image & verify from 1 source up to 4 destinations. Optional Multi-Task feature provides multi-source to multi-target imaging for simultaneous imaging of up to 5 source drives**
- **Optional Targeted/Logical Imaging feature allows you to create a logical image using pre-set, custom filters, file signature filters and/or keyword search to capture only specific files needed**
- **File Browser feature provides write-blocked preview/triage of drive contents**
- **Image from SATA/FireWire®/USB 3.0. IDE & PCIe M.2 SATA/AHCI/ NVMe type SSDs with optional adapters. Optional SAS support available for source and destination with a software option**
- **Capture from a Mac® computer booted in Target Disk Mode using the FireWire port. Supports MacBook Pro® and Mac computers with USB-C ports**

Designed for field or forensic lab use, the Talon® Ultimate delivers advanced, high-performance forensic imaging at a budget-friendly price. Featuring a compact footprint, user-friendly navigation and unbeatable imaging speed it has been engineered specifically for digital forensic investigators, the Talon Ultimate meets all of your forensic imaging, hashing and wiping requirements.

FEATURES

- The Talon® Ultimate is an **extremely fast forensic imaging solution**, achieving speeds of over 40GB/min.
- **Image and verify to multiple image formats;** native copy, .dd image, .dmg image, e01 and ex01. The Talon Ultimate provides SHA1, SHA256, and dual hash (MD5+SHA1) authentication at extremely fast speeds.
- Talon Ultimate formats destination drives to **NTFS, EXT4, FAT 32 or exFAT** file systems. The unit supports imaging from source drives formatted to any major file system.
- **Write-blocked source ports** include 1 SATA (SAS optional), 1 USB 3.0, 1 FireWire®, 1 PCIe. SAS support is enabled via a software option, no additional modules required. 1 additional SATA (SAS optional) source port can be activated with the purchase of the **Multi-Task** option.
- **Destination ports** include 2 SATA (SAS optional), 1 USB 3.0 and 1 FireWire. SAS support is enabled via a software option, no additional modules required.
- **PCIe Support.** Support for imaging from M.2 PCIe (SATA, AHCI, and NVME types), PCIe and mini-PCIe express cards, is available using the Talon Ultimate's PCIe source port and optional adapters.
- **Networking Feature.** Use the Talon Ultimate to image to a network repository using CIFS protocol and/or image from a network repository using iSCSI. Users can use iSCSI as a source or destination drive.
- **Multi-Task option.** This option adds 1 additional **SATA** source port (**SAS optional**) and allows you to image simultaneously from multiple sources to multiple destinations including a network repository. This option also provides support to image one drive while hashing and/or wiping a second drive simultaneously. Users can perform up to 5 tasks concurrently.
- **Concurrent Image+Verify.** Imaging and verifying concurrently takes advantage of destination hard drives that may be faster than the source hard drive. Duration of total image process time may be reduced by up to half.
- **Parallel Imaging.** Perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. Clone to a network location or a destination drive using mirror copy mode while simultaneously imaging in e01 or .dd format to a different destination drive. Requires purchase of Multi-Task option.
- **Targeted/Logical Imaging.** Create a logical image using pre-set, custom filters, file signature filters and/or keyword search to capture only specific files needed. An MFT report can be generated that contains a potential deleted file list. Format output to L01, LX01, ZIP or directory tree. Browse and view directly on the Talon Ultimate display, or use a web browser on a PC that is connected to the same network as the Talon Ultimate. Requires the purchase of the **Targeted Imaging option.**

www.logicube.com
Toll-free (in U.S. only): **888.494.8832** ■ Tel: **818.700.8488** ■ Fax: **818.700.8466**

Logicube

TALON ULTIMATE

A powerful forensic imaging solution with exceptional performance, features & reliability

FEATURES

- **Write-Blocked Drive Preview.** Preview drive contents directly on the Talon Ultimate. The **file browser** feature provides logical access to source or destination drives connected to Talon Ultimate. Users can view the drive's partitions and contents, and view text files, PDF, XML, HTML files.
- **The Talon Ultimate provides built-in support for SATA/USB3/FireWire** storage devices including solid state drives. SAS devices are supported with the purchase of a software option. 2.5"/3.5" **IDE** drives are supported with an adapter included with Talon Ultimate. PCIe, 1.8" IDE, 1.8" ZIF, mSATA, microSATA, eSATA and flash drives are supported with optional adapters.
- Secure sensitive evidence data with whole disk, open standard, drive encryption using the NIST recommended **XTS-AES-256 cipher mode**, decrypt using the Talon Ultimate or open source software such as VeraCrypt.
- **Network Push Feature.** Push evidence files from destination drives connected to the Talon Ultimate or from a Talon Ultimate repository to a network location. The Push feature provides a more secure method than simply copying and pasting to the analysis computer by performing an MD5 or SHA hash during the push process.
- **Users can capture from a Mac® computer** booted in Target Disk Mode using the FireWire port. An off-the-shelf Thunderbolt™ to FW cable is required for Mac computers with a Thunderbolt port. Supports MacBook Pro®, and Mac computers with USB-C ports.
- **Image from a PC/laptop without removing hard drives.** Create a forensic bootable USB flash drive to image a source drive from a computer on the same network without booting the computer's native OS. **Supports Surface Pro 4 and above** laptops.
- **Use the USB3.0 device port to provide write-blocked preview/triage of suspect drives** connected to Talon Ultimate. Users can also copy files from drives to their PC with this feature. **The Talon Ultimate can be used as a write-blocker.**
- **Administrative feature** allows users to save configuration settings and set password-protected user profiles.
- **A web-based user interface** allows users to connect to the device from a web browser and manage all operations remotely. The browser features automatic page scaling for iPad type devices and authentication.
- Features an **internal, removable storage drive** that stores the OS and logs. The drive is easily removed for secure/classified locations.
- **Image from a CD/DVD Blu-Ray.** The Talon Ultimate can image CD/DVD/Blu-Ray media by using a USB optical drive connected to the USB port on the Talon Ultimate. Supports multi-session CD/DVDs.
- **Securely sanitize drives.** Use a custom pass, DoD 7-pass setting or use Secure Erase to wipe drives.
- **Audit Trail/Log files** provide detailed information on each operation. Log files can be viewed on Talon Ultimate or via a web browser, exported to XML, HTML or PDF format to a USB enclosure. Users can print the log files directly from their PC when connected to Talon Ultimate via a web browser.
- **Additional features include** HPA/DCO capture, drive spanning, color touchscreen display, on-screen keyboard, HDMI port, two USB 2.0 host ports for keyboard, mouse or printer connectivity, blank disk check feature, drive trim feature, and detailed information, including S.M.A.R.T. data, on drives connected to Talon Ultimate.

**The Talon Ultimate achieves speeds of over 40GB/min using solid state "suspect" drives that contain a freshly installed Windows XOS and random data. Settings used are EO1/Ex01 image format, using compression and verify "on". The specification and condition of the suspect hard drives as well as the mode, image format and settings used during the imaging process may affect the achieved speeds.*

OPTIONS

- **Multi-Task Option.** Software option activates a 2nd SATA source port (SAS optional). Provides ability to image multiple source drives to multiple destinations simultaneously. Includes 1 SAS/SATA cable
- **SAS Option.** Software option enables SAS support on both source and destination ports
- **Targeted/Logical Imaging Option.** Software option enables a feature that allows you to create a logical image using pre-set, custom filters, file signature filters and/or keyword search to capture only specific files needed
- PCIe adapter kit. Includes adapters for M.2 PCIe, M.2 SATA, M.2 NVMe, mSATA, PCIe and mini-PCIe cards
- USB 3.0 4-port hub
- USB 3.0 to SATA adapter allows you to connect SATA drives to the USB3 ports
- 1.8" IDE to SATA, 1.8" ZIF adapters
- eSATA to SATA cable, mSATA to SATA adapter. microSATA to SATA adapter
- Flash media reader
- 18" extended length SAS/SATA cable set
- Extended 1 year and 2 year warranties
- Soft-sided carrying bag
- Hard case (Pelican type)

IN THE BOX

The Talon Ultimate is shipped in a cardboard carrying case that includes a custom foam insert ready to drop into a standard Pelican hard case

- Power supply & US power cord
- 1 CAT6 network cable
- 4 6-pin SATA power plugs for eSATA drives
- 2.5"/3.5" IDE to SATA adapter
- 1 FireWire cable
- Users' manual on CD-ROM
- 3 SAS/SATA data & power cable
- 1 USB 3.0 device cable

SPECIFICATIONS

Power Requirements	Power Consumption	Operating Temperature	Relative Humidity	Net Weight	Dimensions	Agency Approvals
12 V DC, Grounded 11.5 AMP	<140W w/drives	0-40°C 32 to 104° F	20% to 80%	2.0lbs/1.0k	7.6"W X 5.5"D X 2.6"H (19.0cm X 13.9cm X 6.6cm)	RoHs compliant FCC Part 15 Class A CE

www.logicube.com

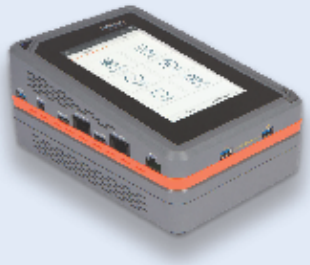
Toll-free (in U.S. only): **888.494.8832** ■ Tel: **818.700.8488** ■ Fax: **818.700.8466**

Logicube

opentext™

What's new in OpenText Tableau Forensic Imager (TX1) 3.0

- Remote access
- Improved efficiency
- Thorough media detail
- Enhanced user experience



OpenText™ Tableau Forensic Imager (TX1) is a highly-intuitive imaging solution that solves the difficult challenges surrounding forensic data acquisition. It offers superior local and networked forensic imaging capabilities with no compromises, even when conducting simultaneous forensic jobs. TX1 delivers consistent results, giving investigators peace of mind when dealing with various types of digital evidence.

Key new features of TX1 3.0

Remote web interface

All features of TX1 3.0's touchscreen user interface (UI) are now available remotely through a web UI when using a modern web browser on a computer, tablet or smartphone. Investigators can manage administration/operation and participate in an investigation from any computer within the same network domain.

Supported web browsers include Google Chrome™, Mozilla® Firefox® and Safari®.

Pause and resume imaging jobs

For the first time in the forensic industry, users can pause any running imaging job (E01, Ex01, DD, DMG) and resume later, even across power-cycles. This increases efficiency by saving time in a variety of scenarios that previously required the job to be restarted.

View Image and Plain Text Files

Users can now view suspect media image and text files directly on TX1 to quickly triage and determine the priority or relevance to the investigation.

- Supported image file extensions include jpg, jpeg, pjpeg, png, apng, gif, jfif, cur, pjp, bmp, ico, svg and webp.
- Supported plain text file extensions include bat, c, conf, csv, h, htm, html, ini, js, json, log, nfo, py, readme, sh, text, tsv, txt and xml.
- When TX1 is connected to a forensic workstation, any additional file types viewable by that workstation are also available.

Display Disk > Partition > File System

Investigators can view a drive's layout of partitions, file systems and raw hex and ASCII data. As a result, users have a more complete view of suspect media and the evidence that might be hidden on it.

opentext™

Multi-user access

Users can now create, delete and manage multi-user profiles, resulting in an improved user experience. This allows users to uniformly deploy common pre-selected settings, as well as personalize or customize individual settings.

Market leader in encrypted drive detection

Additional encrypted drive types are now detected by TX1:

- Opal self-encrypting-drives
- Apple® FileVault® 2
- Check Point® Full Disk Encryption
- McAfee® Drive Encryption (SafeBoot)
- Sophos® Safeguard (Enterprise and Easy/Ultimaco)
- WinMagic® SecureDoc Full Disk Encryption
- GuardianEdge™ Encryption (Plus, Anywhere, Hard Disk Encryption)
- Symantec™ Endpoint Encryption

TX1 also now detects if a drive is part of a RAID set.

Export and import saved logical image searches

The ability to export and import logical image searches significantly improves efficiency and user experience during logical acquisitions. Users can also leverage wildcard characters in search criteria for logical images.

Identify if source drive is part of a RAID

The user can identify if the source drive is part of a RAID, providing thorough media detail and improved efficiency.

Improved user experience

The following new features are included for improved user experience:

- Update time using NTP server.
- Add hostname field to allow easier ID for multi-network systems.
- Display file size after each file in Browse screens.
- Enable firmware update via USB flash drive or any mounted file system.
- Localization updates for changes from TX1 2.2 release.

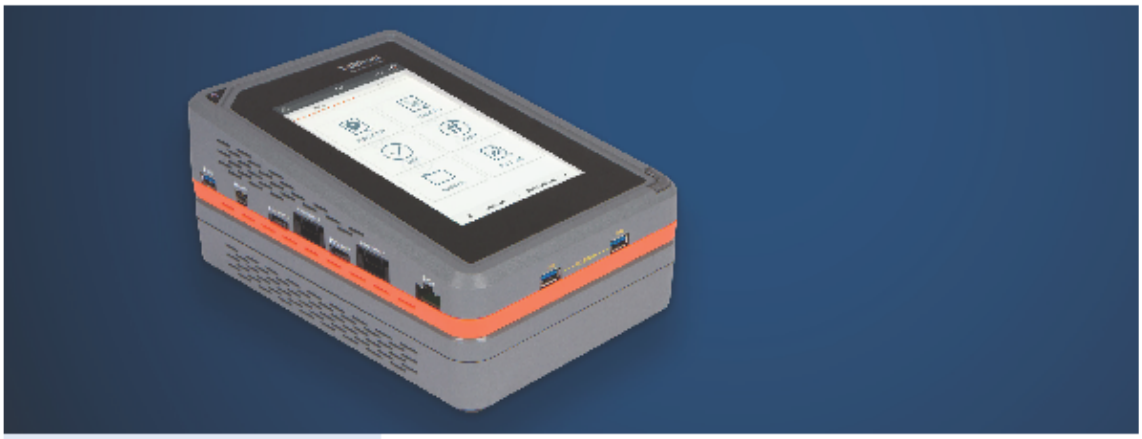
opentext.com/contact Twitter | LinkedIn

opentext™

Product overview

OpenText Tableau Forensic Imager (TX1)

A remarkably versatile and intuitive forensic imaging solution that acquires more data, faster and from more media types, without sacrificing ease-of-use or portability



- **Broad media support**
- **Simultaneous** operations and queuing
- **Superior** local and network imaging performance
- **Beautiful** and intuitive user interface

The increasing diversity, size and sophistication of digital media makes evidence collection a challenge. Digital investigators need a versatile solution that can acquire data from any storage type, including network shares, that is easy to use and navigate and can help close cases faster, reduce case backlogs and increase investigative capacity.

The OpenText Tableau Forensic Imager (TX1) solves the difficult challenges of forensic data acquisition by offering superior local and networked forensic imaging capabilities with no compromises, even when conducting simultaneous forensic jobs. It delivers consistent results, giving examiners and investigators the peace of mind they need when dealing with many types of digital evidence, all within a standalone, high-performance hardware solution.

Broad media support

The TX1 enables full forensic imaging from a wide variety of media, including PCIe, 10Gb Ethernet and Apple® Mac® in Target Disk Mode (USB-C, Thunderbolt and FireWire).

Simultaneous operations and queuing

With the TX1, investigators can expedite cases by conducting two concurrent forensic jobs, anything that involves creating a hash: Logical, Duplicate, Hash, Verify and Restore, and queue additional jobs, without sacrificing performance. Additional scheduled jobs begin as soon as an active job completes.

opentext™

Superior local and network imaging performance

The industry's first 10 GbE connection forensic imager, the TX1 provides unmatched network imaging performance, with little to no drop in performance when simultaneously hashing, encrypting or imaging multiple drives.

Beautiful and intuitive user interface

The TX1 provides an intuitive, informative and easy-to-use UI, all running on a seven-inch, color touch-screen display. It enables examiners of all skill levels to get the job done fast, with minimal to no training.

The TX1 provides digital investigators with unmatched durability, forensic integrity, advanced imaging and performance, all delivered with an intuitive and flexible user experience.

Broad media supported by TX1

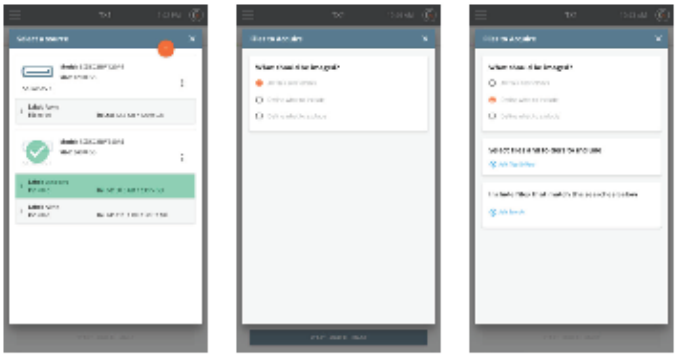
Feature	Description
Logical imaging and search	Acquires logical images from locally attached drives and network shares Collects the entire file system or user can manually select specific folders and files, or use the TX1's powerful search capabilities to define a targeted search profile using pre-defined and custom criteria
Detect drives with whole disk encryption	Automatically detects drives encrypted with the following popular encryption types: Microsoft® BitLocker®, BitLocker To Go, Apple FileVault 2, Linux® LUKS, BestCrypt and Symantec™ PGP™ Disk
Comprehensive Apple Target Disk Mode Forensics	Offers several methods to acquire digital evidence from Mac computers in Target Disk Mode over USB-C, FireWire or Thunderbolt (with Apple's FireWire to Thunderbolt adapter) Captures both physical drives (HDD and SSD) configured as one Fusion Drive on iMac® and Mac Mini®
Up to four destinations per source	Supports up to four destinations per source (1:4) with the ability to mix clone/image duplication and local/network destinations (outputs to SATA, USB 3, SAS and network shares)

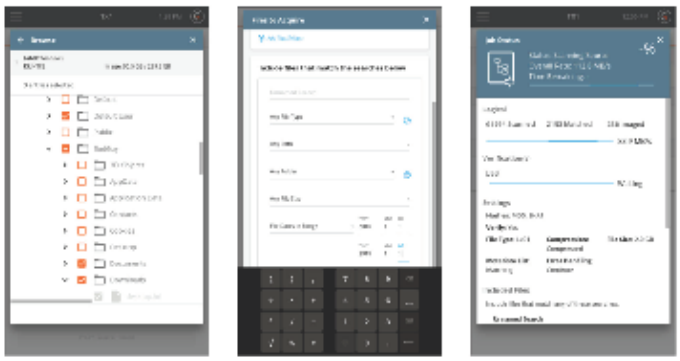
opentext™

Restore image to drive	Restores image files created by the TX1 to a full drive, with its original formatting and directory structure
Acquire from and output to network shares	Acquires from and outputs to many types of network shares (NAS, SAN, domain and workstation shares) using CIFS or iSCSI protocols
10 Gigabit Ethernet	Provides superior network imaging performance over a convenient RJ-45 connection, which is backwards compatible with 1GbE networks
Media utility options	Provides the ability to view extensive drive details, wipe, format, manage Tableau-style drive encryption, view and disable HPA/DCO, blank check, browse filesystem, view SMART data, export as iSCSI target for remote access and eject media
Modular destination drive bay	Includes an optional fan-cooled drive bay (TX1-S1), which provides two cable-less connections for 2.5-inch or 3.5-inch SATA/SAS drives, and when it is connected, examiners can employ up to four simultaneous SATA/SAS destinations
Display more USB device descriptors	Displays the following USB descriptors in the USB drive details screen and reports in the forensic log: VID (Vendor ID), PID (Product ID), class, subclass and protocol

TX1 Logical Imaging in action

TX1 Logical Imaging enables users to save valuable time and destination drive capacity requirements, by focusing on specific files of interest rather than acquiring the entire physical drive.





See the demo

Keep up to date

Learn more

Note: TX1 comes with a three year parts and labor warranty.

opentext.com/contact Twitter | LinkedIn

WiebeTech by CRU

Ditto

Essential for digital investigators

A must-have for digital forensic investigations, the Ditto Forensic FieldStation is a complete and portable toolkit for creating disk clones and images. Ditto FieldStation can be deployed by non-forensics experts and administered and operated remotely by forensics specialists. Via VPN, the Ditto FieldStation can be configured, administered, and managed via an intuitive web browser interface.

FEATURES	BENEFITS
Portable	The Ditto Forensic FieldStation is portable, yet powerful. It travels with or instead of you into the field to create disk clones and images. Ditto FieldStation also helps you log and maintain your chain of custody while using forensic (write-blocked) methods.
Suspect inputs (write blocked)	SATA, eSATA, PATA, USB 2.0, Ethernet (iSCSI, NFS, SMB). Additional interfaces via expansion modules.
Destination outputs	Dual SATA, eSATA (single, dual and mirrored), Ethernet (iSCSI, NFS, SMB), SD Card
LCD navigation	System operation via front panel LCD and soft-touch navigation.
Web browser interface	System configuration, management, and operation via web browser interface. Supports remote preview and operation via network or VPN.
Multi-user support	Web browser can be multi-user password protected, including assignment specific permission levels by user profile.
Drive cleaning	Utility supports nine erase modes including government approved preset modes and user configurable options.
Stealth mode	Turns off LCD display and LED indicators to prevent detection while operating.
Quiet	Rugged, all aluminum design with no fans makes the Ditto FieldStation a durable device that is quiet in all environments.

CRU

POWERFUL DRIVE IMAGING DEVICE

WiebeTech
by CRU

4.92" x 6.77" x 1.72"
(125mm x 172mm x 43.7mm)
Shipping Weight 5 lbs. (2.3kg)

PART NUMBER	DESCRIPTION
31700-2800-0000	Ditto (US plug)
31310-0000-0060	Field Kit D-0, which includes a Ditto Carrying Case and a separate Pelican 1450 case with custom foam designed for Ditto and expansion modules. Ditto and expansion modules sold separately.
31310-2800-0061	Field Kit D-1, which includes a Ditto unit and accessories in a Pelican 1450 case with custom foam. US power cord.

Additional configurations and part numbers for US and international versions available at cru-inc.com/ditto.

Flexibility and speed via browser-based interface
An easy-to-use web browser interface supports remote operation via network or VPN, providing access to Ditto configuration, user administration and user rights, as well as direct operation of Ditto cloning and imaging. This time- and money-saving capability speeds time to data capture, as well as allows organizations to optimize staffing and deployment.

Stand alone use
Work with evidence drives directly from Ditto, with no host computer required, whether in the lab or in the field. The easy-to-use LCD menu makes it simple to view device information, start an image capture or clone a drive.

Easy multi-user management
Separate user or agent profiles, with user-assignable access rights, can be created for Ditto.

Logical imaging
Streamline workflows and shave hours from evidence gathering by using Ditto to quickly navigate through filesystems and image only the files of interest.

Expansion modules
Additional connectivity and input sources are supported with durable metal snap-on modules. Options include USB 3.0, FireWire 800/400, SAS, and media cards.

Data acquisition modes
Clone, DD, E01 with MD5 and SHA-1 hashing. Ditto also has a combined mode that captures a clone and image in a single pass reading of suspect drives.

Log files
Log files are stored on a removable SD card for classified and intelligence applications, so no operational data needs to remain on the Ditto system. XML format allows users to parse data for reports. HTML format makes it easy for users to view information using any web browser.

NetView
Based on Nmap®, Ditto provides detailed information for devices currently attached to the network interfaces.

Multiple file system formats
Supports NTFS, HFS+, XFS, FAT32, EXT4, EXT3, EXT2.

Target mode
Allows Ditto to serve attached drives as iSCSI Target devices via the network interfaces.

CRU

```
Created By AccessData® FTK® Imager 4.2.0.13
Case Information:
Acquired using: ADI4.2.0.13
Case Number: 1
Evidence Number: 1
Unique description: sdsdds
Examiner: sdsdsd
Notes: ssdfsd
---------------------------------------------------------------
Information for D:\Ima\Spooner_Evidence:
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 16.383
 Heads: 16
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 104.857.600
[Physical Drive Information]
 Drive Interface Type: ide
[Image]
 Image Type: VMWare Virtual Disk
 Source data size: 51200 MB
 Sector count:    104857600
[Computed Hashes]
 MD5 checksum:    4689a0c90a229452ce84256a4d5f1321
 SHA1 checksum:   e5781ba29d91fb132f351504598e16f7d749f493

Image Information:
 Acquisition started:   Fri May  8 00:19:27 2020
 Acquisition finished:  Fri May  8 00:39:56 2020
 Segment list:
  D:\Ima\Spooner_Evidence.E01

Image Verification Results:
 Verification started:  Fri May  8 00:40:05 2020
 Verification finished: Fri May  8 00:48:57 2020
 MD5 checksum:    4689a0c90a229452ce84256a4d5f1321 : verified
 SHA1 checksum:   e5781ba29d91fb132f351504598e16f7d749f493 : verified
```

Thesis Case

Autopsy Forensic Report

HTML Report Generated on 2020/05/13 11:41:34

Case:	Thesis_DataLeak
Number of Images:	1

Image Information:

Spooner_Evidence.E01

Timezone:	Europe/Paris
Path:	D:\Image\Spooner_Evidence.E01

Software Information:

Autopsy Version:	4.14.0
Correlation Engine Module:	4.14.0
Data Source Integrity Module:	4.14.0
Email Parser Module:	4.14.0
Embedded File Extractor Module:	4.14.0
Encryption Detection Module:	4.14.0
Exif Parser Module:	4.14.0
Extension Mismatch Detector Module:	4.14.0
File Type Identification Module:	4.14.0
Hash Lookup Module:	4.14.0
Interesting Files Identifier Module:	4.14.0
Keyword Search Module:	4.14.0
PhotoRec Carver Module:	7.0
Plaso Module:	4.14.0
Recent Activity Module:	4.14.0
Virtual Machine Extractor Module:	4.14.0

Ingest History:

Job 1:

Data Source:	Spooner_Evidence.E01
Status:	COMPLETED
Enabled Modules:	Recent Activity Encryption Detection Virtual Machine Extractor Plaso Hash Lookup File Type Identification Embedded File Extractor Exif Parser Keyword Search Email Parser Extension Mismatch Detector Interesting Files Identifier PhotoRec Carver Encryption Detection

Case Summary

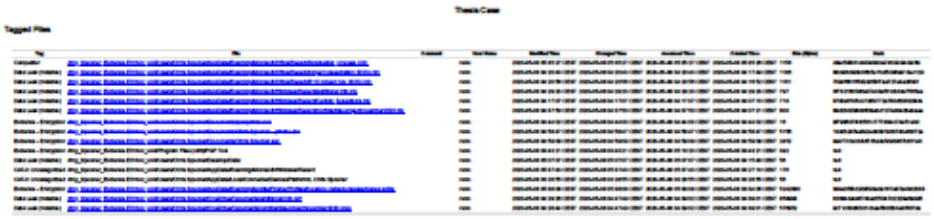
Correlation Engine
Data Source Integrity

Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org

Operating System Information

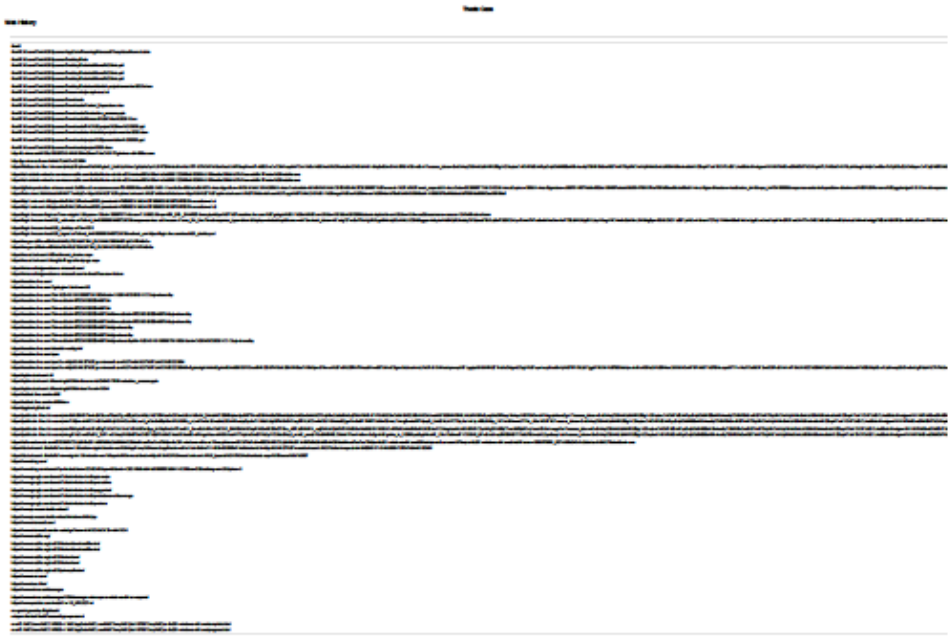
Recent Documents

Tagged Files



Web Downloads

Web History



Web Search

Thesis Case

Web Search

Text	Domain	Date Accessed	Program Name	Source File	Tags
firefox	www.bing.com	0000-00-00 00:00:00	Microsoft Edge	img_Spooner_Evidence.001\vol_vol2\Users\Chris Spooner\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
java jre	www.google.com	2020-05-06 03:38:01 CEST	FireFox	img_Spooner_Evidence.001\vol_vol2\Users\Chris Spooner\AppData\Roaming\Mozilla\Firefox\Profiles\huoslmvs.default-release\places.sqlite	
onedrive	www.google.com	2020-05-06 03:58:32 CEST	FireFox	img_Spooner_Evidence.001\vol_vol2\Users\Chris Spooner\AppData\Roaming\Mozilla\Firefox\Profiles\huoslmvs.default-release\places.sqlite	
mgb test	www.google.com	2020-05-06 03:43:03 CEST	FireFox	img_Spooner_Evidence.001\vol_vol2\Users\Chris Spooner\AppData\Roaming\Mozilla\Firefox\Profiles\huoslmvs.default-release\places.sqlite	
windows office mega	www.google.com	2020-05-06 03:44:33 CEST	FireFox	img_Spooner_Evidence.001\vol_vol2\Users\Chris Spooner\AppData\Roaming\Mozilla\Firefox\Profiles\huoslmvs.default-release\places.sqlite	
winrar	www.google.com	2020-05-06 03:45:01 CEST	FireFox	img_Spooner_Evidence.001\vol_vol2\Users\Chris Spooner\AppData\Roaming\Mozilla\Firefox\Profiles\huoslmvs.default-release\places.sqlite	